STRANGE DÉJÀ VU: TACKLING INFORMATION SHARING PROBLEMS FOR EFFORTS AGAINST TRANSNATIONAL ORGANIZED CRIME

BY

CHRISTOPHER W. ALLEN

A THESIS PRESENTED TO THE FACULTY OF

THE SCHOOL OF ADVANCED AIR AND SPACE STUDIES

FOR COMPLETION OF GRADUATION REQUIREMENTS

SCHOOL OF ADVANCED AIR AND SPACE STUDIES

AIR UNIVERSITY

MAXWELL AIR FORCE BASE, ALABAMA

JUNE 2015

DISCLAIMER

The conclusions and opinions expressed in this document are those of the author. They do not reflect the official position of the US Government, Department of Defense, the United States Air Force, or Air University.

ABOUT THE AUTHOR

Major Christopher W. Allen (BA, University of Louisville; JD, University of Louisville; MA, Naval Postgraduate School; MA, Air Command and Staff College) is a student at the School for Advanced Air and Space Studies, Maxwell AFB, Alabama. As a special agent in the Air Force Office of Special Investigations (AFOSI), he holds extensive experience in counterintelligence, counter-threat operations, and felony-level criminal investigations. Maj Allen has commanded five detachments stateside and deployed, including the largest detachment in Afghanistan, AFOSI Expeditionary Detachment 2405, and AFOSI Detachment 241, Al Udeid AB, Qatar. He also served as Operations Officer for AFOSI 24th Expeditionary Field Investigations Squadron, Al Udeid AB, Qatar, where he traveled extensively to support AFOSI units in Iraq, Afghanistan, Jordan, Kuwait, United Arab Emirates, and Kyrgyzstan. Maj Allen is an honors graduate of the Arabic program at the Defense Language Institute, Presidio of Monterey, California, and a graduate of the Middle East Security Studies program at the Naval Postgraduate School, Monterey, California. He is a graduate of USAF Air Command and Staff College, Squadron Officer School, Aerospace Basic Course, and Officer Training School. Maj Allen is a Distinguished Graduate of the AFOSI Special Investigations Academy, Federal Law Enforcement Training Center, Glynco, Georgia. Prior to cross-training into AFOSI, he served as an Acquisitions Manager with oversight for various Chemical/Biological Defense programs. Though non-practicing, Maj Allen remains a licensed attorney in the Commonwealth of Kentucky.

ACKNOWLEDGMENTS

I would like to recognize several individuals who have been crucial to the successful completion of this study. I want to thank Colonel Howard Jones for his insightful guidance, infinite patience, and good humor that led me to the successful completion of this project. Thanks also to Doctor James Kiras, Doctor James Tucci, and Colonel Richard Bailey for their fantastic support and very constructive advice that helped channel and refine my research. I also want to express my appreciation to Katherine M. Bukolt, SES, for her generous assistance early in the research process to orient me to relevant subject matter.

I especially want to thank Colonel (Retired) Terry McCaffrey and Colonel Terry Bullard for their unwavering support and mentorship throughout this effort. I also want to acknowledge Special Agent Rick Munck for his willingness to share contacts and much-appreciated service as a sounding board for my ideas.

Most importantly, I want to express my sincere and deep appreciation to my family and friends for their love, patience, and understanding when I was absent in mind, body, or spirit, due to the time needed to research and produce this paper. Their presence and unwavering support was very important to me and made all the difference in ensuring the successful completion of this work.

ABSTRACT

This study identifies and analyzes information sharing problems in United States (US) government efforts to combat transnational organized crime, as well as analogous US counterterrorism efforts, using a composite framework: a combination of Alfred Chandler's notions of *strategy* and *structure* with Edgar Schein's ideas on *organizational culture*. Specifically, this study examines key US government and Department of Defense (DOD) strategy documents and select organizations relevant to DOD involvement in information sharing efforts against transnational organized crime, and analyzes specific post-9/11 counterterrorism entities for insights that may help DOD and other agencies avoid information sharing issues in the fight against transnational organized crime. The author argues the US government—and DOD in particular—must synchronize strategy, structure, and culture in order to solve information sharing problems with efforts to combat transnational organized crime. DOD must understand the capabilities and limitations of information sharing throughout federal, state, and local government levels—as well as DOD's own information sharing capabilities and limitations with external partners. Recommendations for the US government and DOD to consider to posture resources to confront an identified national security threat more effectively include: (1) improvement of existing strategy, structure, and culture to enhance information sharing for a decentralized enterprise against transnational organized crime, or (2) if forced by a catastrophic event, creation of an integrated, operational task force for homeland protection against transnational organized crime.

CONTENTS

Chapter 1

Introduction

Background

Organized crime is not a new phenomenon, nor is the conduct of criminal activities across international borders. Banditry and piracy are arguably the oldest forms of organized crime. Across millennia, bandit gangs in diverse parts of the world have ignored societal rules and traversed established land boundaries in order to locate lucrative targets for criminal predation. Likewise, pirates commandeered ships, looted valuable cargo, and kidnapped or enslaved crews on the high seas and in littoral areas around the globe in violation of maritime custom and laws. Pirates operated land bases, sometimes in multiple countries, in order to trade seized currency, goods, and captives for logistical support and sanctuary. Contemporary banditry and piracy remain menacing versions of organized crime, fundamentally unchanged over the centuries.

Yet, at least for Americans, reference to organized crime is more likely to conjure up images of Al Capone or other gangsters of the early twentieth century who defied Prohibition and law enforcement at all levels of government, rather than pirates and bandits. While "rum runners" at sea and "bootleggers" on land smuggled alcohol into the United States (US) from the Caribbean, Europe, and Canada in the 1920s and 1930s, powerful criminal syndicates with significant ties to Italy—specifically, the Sicilian Mafia—distributed alcohol within the US and engaged in numerous other illegal activities, including firearms and drug trafficking, money laundering, prostitution, gambling, corruption, extortion, kidnapping, assault, and murder. Today, worldwide earnings for Italian organized crime may exceed $100 billion annually. Despite decades of investigations and prosecutions, the Federal Bureau of Investigation (FBI) considers the American Mafia, "the foremost organized criminal threat to American society."[1]

While organized crime equates typically with "the Mob" in the minds of US policymakers and law enforcement, Latin American narcotics traffickers with extensive distribution networks between bases in Central and South America and street corners

[1] Federal Bureau of Investigation, "Italian Organized Crime," http://www.fbi.gov/about-us/investigate/organizedcrime/italian_mafia (accessed 3 December 2014).

throughout America no less engage in other types of organized crime across international borders. Since the 1970s, Latin American drug cartels grew to rival legitimate multi-national corporations in terms of organization and sophistication.[2] The US government has waged a two-front "War on Drugs" against the cartels: an anti-drug information and treatment campaign to reduce the demand for drugs in the US and significant law enforcement and military efforts to interdict the drug supply and pursue the arrest and prosecution of suppliers. Unfortunately, as long as the demand in the US for drugs produced in Latin America (e.g., cocaine, marijuana, methamphetamines) remains, Latin American drug cartels will continue to garner profits and pose an instability and corruption threat for states where they operate. The same threat appears in other parts of the world with drug trafficking organizations and other criminal organizations involved in various types of crime, including those based in formerly closed societies.

The end of the Cold War in the early 1990s witnessed the opening of societies through democratic transition and the expansion of capitalism and trade to previously-closed markets. Political and economic reforms in numerous states, along with the spread of globalization, increased the movement of goods, information, and people across borders—positive developments for human rights, global commerce, and trade. At the same time, these positive developments offered opportunities for exploitation. Arguably inseparable from legitimate globalization, the term "deviant globalization" captures how "entrepreneurs use the technical infrastructure of globalization to exploit gaps and differences in regulation and law enforcement of markets for repugnant goods and services."[3] Traffickers of various types transport drugs, weapons, humans, counterfeit goods and currency, etc., to markets all over the world via the international commercial shipping system, criminal organizations leverage diverse international financial institutions to hold and transfer funds necessary for operations, and cyber-savvy criminals exploit legitimate online capabilities to identify, coordinate, and track business deals, while also taking advantage of government, corporate, and individual online

[2] Jennifer L. Hesterman, "Transnational Crime and the Criminal-Terrorist Nexus: Synergies and Corporate Trends" (Master's thesis, Air University, April 2004), 5-6.
[3] Nils Gilman, Jesse Goldhammer, and Steven Weber, "Deviant Globalization," in *Convergence: Illicit Networks and National Security in the Age of Globalization*, ed. Michael Miklaucic and Jacqueline Brewer (Washington: National Defense University Press, 2013), 3.

vulnerabilities to commit fraud and virtual theft. In short, globalization and the opening of societies and markets increased possibilities for trade and profit, both licit and illicit.

Problem and Relevance

In recent decades, policymakers and analysts in the US and around the world increasingly discussed and analyzed the problem of "transnational organized crime." If it lacks novelty as a phenomenon, then what explains the increased attention on organized crime that crosses state boundaries in order to maximize profits? More recent attention given to transnational organized crime stems from concerns over the proliferation and diversity of criminal organizations since the end of the Cold War in conjunction with the spread of globalization.[4] For example, Russian and other Eastern European criminal groups grew in fertile soil created in states struggling to transition from communist systems to capitalist democracy in the 1990s—where "crime came to permeate society and politics"—and evolved into powerful transnational organizations involved in a multitude of illicit activities.[5] For good reason, policymakers and analysts view unprecedented illegal monetary gains and negative influential power of transnational criminal organizations as trends that must be halted and reversed. Though estimates vary greatly, it is likely that direct (illegal profits) and indirect (political/societal impact) economic losses to illicit trade number in the hundreds of billions of dollars annually.[6]

Identification of a "crime-terror nexus," "crime-terror continuum," or "crime-terror-insurgency nexus," with potential or actual links or mergers among criminal, terrorist, or insurgent organizations, also provides a rationale to treat criminal activities as

---

[4] Tamara Makarenko, "The Crime-Terror Continuum: Modelling 21st Century Security Dynamics" (PhD diss., University of Wales, Aberystwyth, 31 March 2005), 17-21. Joseph Nye and David Welch describe globalization as a process that creates networks of interdependence around the world. Enablers of globalization include technological advances that accelerate communications and transportation, and political environments that provide security, regulatory stability, and openness to trade and investment. See Joseph S. Nye, Jr., and David A. Welch, *Understanding Global Conflict and Cooperation: An Introduction to Theory and History*, 9th ed. (Boston: Pearson, 2013), 255, 275, 287.

[5] Svante Cornell and Michael Jonsson, ed., *Conflict, Crime, and the State in Postcommunist Eurasia* (Philadelphia: University of Pennsylvania Press, 2014), 18.

[6] Justin Picard tallies an estimated annual impact of $1.5 trillion for five illegal markets (illegal drugs, human trafficking, excised goods, environmental crimes, and counterfeits), with an annual total market size for the illegal markets valued at $300 billion. See Justin Picard, "Can We Estimate the Global Scale and Impact of Illicit Trade?" in *Convergence*, ed. Miklaucic and Brewer, 51-52, 57-58.

national security threats, not simply routine law enforcement matters.[7] In failed states and ungoverned spaces, criminal organizations threaten permanent corruption and instability. Even worse, criminal support for terrorists—in conjunction with or in lieu of state sponsorship—enables the creation and protection of safe havens for training, planning, and launching terrorist attacks. Decades-long conditions in Afghanistan and Somalia exemplify how different combinations of crime, terrorism, and insurgency pose intractable problems that contribute to difficulties in state development and governance with repercussions for the international security environment. In the post-9/11 world, this is a complex threat the US and its allies and partners are unwilling to ignore.

For the US specifically, a major challenge in confronting the transnational organized crime threat is to share information on actors and activities to enable relevant agencies to pursue suitable measures in a timely manner. According to a senior Department of Defense (DOD) official, the US presently lacks a "robust system for effective, efficient information sharing" among federal law enforcement, intelligence, and military organizations on transnational organized crime threats. Concerns over vertical "stove-piping" of threat information, instead of an effective horizontal cross-flow, persist over a decade after identification of this issue as a critical failure in counterterrorism efforts prior to the 9/11 attacks.[8] An additional concern is that increased competition in a reduced federal budgetary environment in recent years exacerbates bureaucratic "turf battles" over areas of responsibility and related funding, de-incentivizing information sharing among federal agencies that value information as a bargaining commodity. In contrast to the initial years after 9/11, federal law enforcement, intelligence, and military organizations flush with "Global War on Terror" funding created numerous institutions and processes in efforts to remedy pre-9/11 counterterrorism information sharing problems, including creation of the Department of Homeland Security, Office of the

[7] Louise I. Shelley et al., *Methods and Motives: Exploring Links between Transnational Organized Crime & International Terrorism* (Washington: Department of Justice, 23 June 2005), 5-6; Makarenko, "The Crime-Terror Continuum," 168, 184-188; *Strategy to Combat Transnational Organized Crime: Addressing Converging Threats to National Security* (Washington: The White House, July 2011), 6.

[8] *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States* (Washington: National Commission on Terrorist Attacks Upon the United States, 2004), 403, 418.

Director of National Intelligence, and dozens of Joint Terrorism Task Forces in cities across the US. Officials pushed a major cultural shift from information sharing based on a "need to know" to a "need to share."[9] Post-9/11 institutions and processes, and the intended cultural shift, have been tested by experience and scrutinized in the public arena through Congressional oversight, media queries, and academic debate, allowing for identification of lessons learned (or not) for counterterrorism information sharing.

Terrorism and transnational organized crime are distinct national security threats. Yet similarities exist in the ways and means used by terrorist and criminal actors, so much so that policymakers and analysts remain concerned about increased dangers from the "convergence" of terrorist and transnational organized crime threats.[10] If terrorism and transnational organized crime are similar—if not always related—security threats, then efforts to combat them should be similar. It follows that strategic, structural, and cultural innovations to improve information sharing for counterterrorism efforts might hold value for tailored application to information sharing problems with transnational organized crime threats.

Methodology

This study reviews key strategy documents to establish baseline guidance for US national and DOD approaches to combating transnational organized crime and sharing information. Strategic guidance is then compared to specific relevant institutions and processes established to execute the guidance in order to determine whether they align properly and perform efficaciously. This study identifies and analyzes information sharing problems in US efforts to combat transnational organized crime, as well as analogous US counterterrorism efforts, using a composite framework: a combination of Alfred Chandler's notions of *strategy* and *structure* with Edgar Schein's ideas on *organizational culture*. Collectively, relevant strategies and plans should provide clear direction, useful guidance, and prioritization of effort toward the goal of improving

[9] Andrew W. Green, "It's Mine! Why the US Intelligence Community Does Not Share Information" (Master's thesis, Air University, School of Advanced Air and Space Studies, July 2005), 19-20; David L. Carter and Jeremy G. Carter, "The Intelligence Fusion Process for State, Local and Tribal Law Enforcement," *Criminal Justice and Behavior* 36, no. 12 (December 2009): 20-21.

[10] *Strategy to Combat Transnational Organized Crime*, cover letter by President Barack Obama; Miklaucic and Brewer, *Convergence*, xiv-xvi.

information sharing on transnational organized crime. To translate strategies into reality requires proper structures—institutions, or organizations, with appropriate personnel, processes, and infrastructure—to conduct activities in accordance with strategic direction. Yet, without effective leadership and management, strategies are merely words on paper and structures are machines without an operator. Effective leaders develop and refine an organization's culture to motivate personnel continually to pursue strategic goals and to enhance the organizational structure for optimal pursuit of strategic goals. Theoretically, solutions to information sharing problems with transnational organized crime lie in ensuring the presence of sound strategy, effective structures to implement the strategy, and organizational cultures that embrace the strategy and fully leverage structural resources to achieve strategic goals. Where these elements are identified as lacking or missing is most likely where the need for improvement exists, and identification of problems is the first step toward improvement.

This study argues the US government—and DOD in particular—must synchronize strategy, structure, and culture in order to solve information sharing problems with efforts to combat transnational organized crime. The US should leverage lessons learned from counterterrorism efforts to improve information sharing, but leaders and members of relevant organizations must recognize both similarities and differences between efforts against transnational organized crime and terrorism. Since legal, operational, technological, bureaucratic, and cultural "frictions" impede ideal information sharing, responsible entities must comprehend and navigate these issues in order to posture resources effectively to obtain and share information related to transnational organized crime for exploitation by appropriate authorities. For DOD in particular, it must embrace its support function in this fight. DOD is the designated "single lead agency for detection and monitoring of aerial and maritime transit of illicit drugs into the United States."[11] Yet, due to the legal prohibition against use of the US military to enforce domestic laws and sensitivity to sovereignty concerns of partner nations, "DoD's role is almost always to provide unique and tailored support to law enforcement agencies

[11] *Department of Defense Counternarcotics & Global Threats Strategy* (Washington: Deputy Assistant Secretary of Defense for Counternarcotics & Global Threats, 27 April 2011), 11.

and our foreign partners."[12] If it takes "a network to defeat a network," and a network is only as strong as its component parts, DOD must understand the limitations of information sharing throughout federal, state, and local government levels—as well as DOD's own internal limits on information sharing with external partners—in the fight against transnational organized crime.[13] Armed with this understanding, DOD will best be able to craft strategies, enhance or create structures, and foster an appropriate culture to facilitate the timely flow of transnational organized crime information among pertinent partners to combat a growing national—and transnational—security threat effectively.

Limitations and Assumptions

This study does not discuss or include any classified or law enforcement sensitive information in order to make the analysis and findings contained herein as widely accessible as possible to interested audiences, including US federal law enforcement, intelligence, and military personnel. To provide maximum accessibility precludes use of potentially useful examples of successes or failures that remain classified or restricted in dissemination due to concerns in the law enforcement or intelligence communities for protection of sources and methods, on-going investigations or operations, etc.

Another limitation involves scope. This study discusses information sharing problems in the fight against transnational organized crime to provide recommendations for improvement to the US federal level of government, including DOD. As transnational organized crime requires a "whole-of-government" approach, efforts to combat this threat must necessarily involve law enforcement agencies at state and local levels in the US. Therefore, this study includes discussion of various institutions and processes that include state and local participation. Yet, the focus remains on providing solutions to information sharing problems at the federal level. This study also excludes information sharing problems with transnational organized crime at the international level. Problems with sharing information with allies and partners on threats—

[12] William F. Wechsler, Deputy Assistant Secretary of Defense for Counternarcotics and Global Threats, Department of Defense (address, The Washington Institute for Near East Policy, Washington, 26 April 2012).

[13] Stanley A. McChrystal, "It Takes a Network: The New Front Line of Modern Warfare," *Foreign Policy*, 21 February 2011, http://foreignpolicy.com/2011/02/21/it-takes-a-network/ (accessed 14 January 2015).

transnational organized crime or otherwise—offer more than enough material and interest to justify a separate study from this vantage point, especially in relation to DOD efforts.

Chapter Outline

Chapter Two defines key terms for this study, including *transnational organized crime* and *information sharing*, and explains the theoretical framework used in this study—Chandler's notions of *strategy* and *structure* and Schein's ideas on *organizational culture*. Chapter Three analyzes key US government and DOD strategy documents on transnational organized crime and information sharing to identify issues with guidance that cause problems in policy implementation and execution, and to discern any organizational culture elements (i.e., espoused beliefs and values, basic underlying assumptions) or change that relevant strategy documents seek to promote. Chapter Four analyzes select organizations pivotal to DOD involvement in information sharing efforts against transnational organized crime to determine if "structure follows strategy" in accordance with Chandler's thesis, and to identify organizational culture elements or change that relevant structures represent and promote.[14] Chapter Five examines specific post-9/11 domestic counterterrorism entities which offer strategy, structure, and culture insights that may help DOD and other relevant agencies avoid information sharing pitfalls in the fight against transnational organized crime. Chapter Six reviews key findings from this study's analysis of strategy, structure, and culture in relation to information sharing in US efforts to combat transnational organized crime, as well as analysis of information sharing by US counterterrorism entities. Recommendations stem from the findings and seek to improve information sharing in terms of strategy, structure, and culture. More specifically, recommendations offer the US government in general and DOD in particular two options to consider to posture resources to obtain and share information related to transnational organized crime more effectively for exploitation: (1) improvement of existing strategy, structure, and culture to enhance information sharing for a decentralized enterprise against transnational organized crime, or (2) if forced by a catastrophic event, creation of an integrated, operational task force for homeland protection against transnational organized crime.

[14] Alfred D. Chandler, Jr., *Strategy and Structure: Chapters in the History of the Industrial Enterprise* (Cambridge: The M.I.T. Press, 1962), 14.

Chapter 2

Definitions and Theoretical Framework

Defining key terms promotes consistency and clarity for subsequent usage and previews areas for later analysis based on differing definitions of terms. Similarly, explaining the theoretical framework of this study fosters understanding of subsequent analysis and scrutiny of specific issues. Therefore, this chapter defines *transnational organized crime, information sharing,* and related terms first and then discusses Alfred Chandler's *strategy* and *structure* and Edgar Schein's *organizational culture*.

Definition of *Transnational Organized Crime*

While the US definition (discussed subsequently) is binding for purposes of this study, the United Nations (UN) "definition" of transnational organized crime highlights the challenge in defining what appears to be a simple concept. In fact, the 2003 *United Nations Convention Against Transnational Organized Crime* lacks an explicit definition of transnational organized crime. Instead, to arrive at an indirect definition requires a formulaic combination of other defined terms in accordance with the expressed scope of the Convention. The Convention applies "to the prevention, investigation and prosecution" of participation in an organized criminal group, laundering of criminal proceeds, corruption, obstruction of justice, and "serious crime … where the offence is transnational in nature and involves an organized criminal group." A serious crime is an offense punishable by at least four years confinement. An organized criminal group consists of a "structured group of three or more persons" that commits serious crime to obtain financial gain. An offense is transnational if committed in multiple states; if committed in one state but orchestrated from another state; if committed in one state by an organized criminal group that operates in multiple states; or if committed in one state with "substantial effects" in another state.[1] A 2010 UN Office on Drugs and Crime (UNODC) threat assessment notes the Convention's lack of a definition for transnational organized crime or a specific list of crimes encompassed by the phenomenon. The

[1] *United Nations Convention Against Transnational Organized Crime and the Protocols Thereto* (Vienna, Austria: United Nations Office on Drugs and Crime, 2004), 5-6.

UNODC explains that lack of a definition allows for flexibility to address "new forms of crime [that] emerge constantly as global and local conditions change over time."[2]

In contrast to the UN, current US policy provides a definition of transnational organized crime. In the 2011 *Strategy to Combat Transnational Organized Crime*, the Obama Administration states, "**Transnational organized crime** refers to those self-perpetuating associations of individuals who operate transnationally for the purpose of obtaining power, influence, monetary and/or commercial gains, wholly or in part by illegal means, while protecting their activities through a pattern of corruption and/or violence, or while protecting their illegal activities through a transnational organizational structure and the exploitation of transnational commerce or communication mechanisms" (emphasis in original).[3] This definition is the same as the definition of international organized crime provided in the US Department of Justice *Overview of the Law Enforcement Strategy to Combat International Organized Crime* from 2008, except for a clause added at the end by the Obama Administration: "or while protecting their illegal activities through a transnational organizational structure and the exploitation of transnational commerce or communication mechanisms."[4] This addition might explain the adoption of *transnational* over *international*, above and beyond substitution of the latter by the former throughout the definition. However, the Obama Administration does not state this explicitly; instead, it insists the change "more accurately describes the converging threats we face today." "Converging threats" refers to the concern for threats from a "crime-terror-insurgency nexus."[5] While this is a justifiable concern, the change may have been made to align terminology with the UN and member states, or to reflect the nuanced preference for the prefix *trans-* (across or beyond) over *inter-* (between or among) when describing criminal organizations that operate across or beyond the sovereign borders of states, outside the recognized community among states.

While the UN omits a precise definition of transnational organized crime, the Obama Administration's definition actually defines transnational criminal *organizations*,

---

[2] *The Globalization of Crime: A Transnational Organized Crime Threat Assessment* (Vienna, Austria: United Nations Office on Drugs and Crime, 2010), 25.
[3] *Strategy to Combat Transnational Organized Crime*, i.
[4] *Strategy to Combat Transnational Organized Crime*, i.
[5] *Strategy to Combat Transnational Organized Crime*, 3, 6.

not *crime*: "Transnational organized crime refers to those self-perpetuating associations of individuals who operate transnationally."[6] The definition does not specify crimes, rather it identifies actors. The rationale for framing the definition this way may be to expand the focus from specific crimes to the overall threat. Beyond the definition, the Obama Administration identifies ten topic areas for its threat-based notion of transnational organized crime: Penetration of State Institutions, Corruption, and Threats to Governance; Threats to the Economy, U.S. Competitiveness, and Strategic Markets; Crime-Terror-Insurgency Nexus; Expansion of Drug Trafficking; Human Smuggling; Trafficking in Persons; Weapons Trafficking; Intellectual Property Theft; Cybercrime; and the Critical Role of Facilitators (e.g., attorneys, accountants).[7] To illustrate how expansive this notion of transnational organized crime is compared to typical practice, US federal law enforcement agencies tend to distinguish among crimes involving traditional organized crime, drug trafficking organizations, and gangs.[8] The Obama Administration's notion of transnational organized crime eliminates the distinction.

Another observation for the Obama Administration's definition of transnational organized crime is the order of purpose: "power" and "influence" precede "monetary and/or commercial gains." That this definition places pursuit of power and influence ahead of profit in the minds of criminals may reflect a purposeful intent to reorient efforts against transnational criminal organizations toward a broader focus on threats posed to the US and other states, and effects on societies, instead of a narrow focus on investigation and prosecution of individuals for illegal money-making activities.

DOD addresses transnational organized crime and transnational criminal organizations within one definition, stating both "refer to a network or networks structured to conduct illicit activities across international boundaries in order to obtain financial or material benefit. Transnational organized crime harms citizen safety, subverts government institutions, and can destabilize nations."[9] In contrast to the White House's reference to "self-perpetuating associations of individuals," DOD identifies

---

[6] *Strategy to Combat Transnational Organized Crime*, i.
[7] *Strategy to Combat Transnational Organized Crime*, 5-8.
[8] Kristin M. Finklea, *Organized Crime in the United States: Trends and Issues for Congress*, CRS Report R40525 (Washington: Congressional Research Service, 22 December 2010), 3, note 6.
[9] *DOD Counternarcotics & Global Threats Strategy*, 4.

structured networks as the concerning actors involved in transnational organized crime. Additionally, the DOD definition makes no mention of "power" or "influence," unlike the Obama Administration's definition of transnational organized crime. Granted, the DOD definition preceded that of the Obama Administration by less than three months; still, it highlights how definitions for key national security terms can differ at the highest policy levels of the US government, introducing confusion for subordinate agencies.

Current US definitions of transnational organized crime are policy statements, subject to change by subsequent presidential administrations, lacking the force or endurance of federal law. While multiple criminal activities fall under the *conceptual* umbrella of transnational organized crime, there is no *statutory* definition of "organized crime" in US federal law.[10] Though enabling flexibility to adapt to evolving transnational organized crime threats at a policy level, the lack of a legal definition and statutory roles and responsibilities approved by Congress creates long-term planning, resourcing, and accountability issues for US government agencies fighting transnational organized crime. Nevertheless, the White House expects executive agencies to share information on the threat based on policy in the absence of firmer legal guidance.

In addition to the lack of statutory guidance, deficient information sharing among federal law enforcement agencies may stem from "structuring organized crime investigations around the alleged crimes," (violations) instead of around targeted criminal organizations (actors), which "can lead to inter-agency conflicts," over jurisdiction and resourcing to combat specific violations instead of optimal collaboration against actors.[11] Jerome Bjelopera and Kristin Finklea note that transnational criminal organizations may conduct various activities that do not adhere necessarily to the rigid jurisdictional boundaries of federal, state, and local law enforcement agencies. For example, drug, weapons, and human trafficking violations committed by members of a criminal group fall simultaneously under the jurisdiction of the Drug Enforcement Administration, Bureau of Alcohol, Tobacco, Firearms and Explosives, and Immigrations and Customs

[10] Jerome P. Bjelopera and Kristin M. Finklea, *Organized Crime: An Evolving Challenge for U.S. Law Enforcement*, CRS Report R41547 (Washington: Congressional Research Service, 6 January 2012), 34, 36.
[11] Bjelopera and Finklea, *Organized Crime*, 38.

Enforcement, not to mention state and local counterpart agencies.[12] Ideally, agencies with jurisdiction over specific criminal violations will share information to maximize charges and prosecutions against a criminal group's individual actors. When this does not occur, the result can be loss of investigative opportunities to degrade and dismantle transnational criminal organizations. As exemplified in debates pre- and post-9/11 over terrorism as a law enforcement or national security problem, a focus on violations (law enforcement) is different from a focus on threats posed by actors (national security). In the former investigation and prosecution have primacy, while in the latter mitigation and elimination are more important. Arguably like terrorism, transnational organized crime represents a merger of the two foci, creating gray areas wherein law enforcement, intelligence agencies, and the military struggle to sort out how best to share information on violations and actors to destroy the organizations.

Definition of *Information Sharing*

To be required or motivated to share information first necessitates a definition of *information*. DOD defines information as "any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual forms."[13] A simple definition of information is "anything that can be known, regardless of how it may be discovered."[14] Simpler still, information is acquired knowledge. Acquisition of knowledge provides an amount of information, but it does not translate automatically into a general or specific understanding based on context, or usefulness. To gain understanding or usefulness requires processing, analysis (or exploitation), and dissemination of information to others for further processing and analysis (to convert information into intelligence).

Essentially, dissemination of information equates to information sharing. The 2012 *National Strategy for Information Sharing and Safeguarding* does not define information sharing but asserts information is a "national asset" that must be shared and

---

[12] Bjelopera and Finklea, *Organized Crime*, 38.
[13] Department of Defense Directive (DODD) 8000.01, *Management of the Department of Defense Information Enterprise*, 10 February 2009, 10.
[14] Mark M. Lowenthal, *Intelligence: From Secrets to Policy*, 2nd ed. (Washington: CQ Press, 2003), 1-2.

protected in the interests of national security.[15] Fortunately, DOD defines information sharing as, "**'Making information available to participants (people, processes, or systems).'** Information sharing includes the cultural, managerial, and technical behaviors by which one participant leverages information held or created by another participant" (emphasis in original). Methods and means used to share information are "vast, ranging from face-to-face interactions to real-time voice communications, to the latest messaging and data technologies that pass information across trusted networks."[16] Technological change affects information sharing capabilities, but it is important to recognize that policy guidance and cultural norms change over time also (if more slowly) and affect transmission of information in person or across various media. DOD's reference to "people, processes, or systems" and "cultural, managerial, and technical behaviors" connects nicely to the theoretical framework for analysis of information sharing problems in efforts against transnational organized crime: strategy, structure, and culture.

Chandler's *Strategy* and *Structure*

Strategies and plans should provide clear direction, useful guidance, and prioritization of effort toward the goal of improving information sharing on transnational organized crime. Turning strategies into reality requires proper structures—institutions with appropriate personnel, processes, and infrastructure—to conduct activities in accordance with strategic direction. This study borrows notions of *strategy* and *structure* from Alfred Chandler's economic histories to analyze key US strategy documents and relevant institutions for information sharing on transnational organized crime.

Chandler's 1962 historical analysis of modern US business administration is titled, *Strategy and Structure*. In this authoritative work, Chandler traces the development of the "'decentralized' form of organization in American industry" through comparison of the organizational experiences of DuPont, General Motors, Standard Oil, and Sears with nearly one hundred other large industrial enterprises.[17] To facilitate his analysis, Chandler defines strategy as "the determination of the basic long-term goals and

[15] *National Strategy for Information Sharing and Safeguarding* (Washington: The White House, December 2012), 1, 7.
[16] *Department of Defense Information Sharing Strategy* (Washington: Department of Defense Information Sharing Executive, Office of the Chief Information Officer, 4 May 2007), ii, 3-4.
[17] Chandler, *Strategy and Structure*, 2-4.

objectives of an enterprise, and the adoption of courses of action and the allocation of resources necessary for carrying out these goals." In a word, strategy is a vision—a vision expressed in words and ideally captured in writing. Chandler defines structure as "the design of organization through which the enterprise is administered. It includes, first, the lines of authority and communication between the different administrative offices and officers and, second, the information and data that flow through these lines of communication and authority." In addition to the mental processes, skills, and responsibilities of an enterprise, structure includes the necessary physical infrastructure (e.g., factories, offices, communications links) and equipment, financial means, and materials to produce an enterprise's products.[18] In short, structure includes the plan, processes, and means to execute the vision or strategy.

One illustration of Chandler's notions of strategy and structure is DuPont ownership decisions in 1902 to pursue a strategy of consolidation through a centralized administrative structure that eliminated "costly duplication of facilities and personnel" and allowed various corporate functions to "be economically and systematically supervised, and the essential coordination between functions maintained."[19] In so doing, the DuPont family avoided sale of an explosives company already in existence for 100 years and continued its pursuit of profits. Another example of the interaction of strategy and structure is the Sears Company's shift in the 1920s away from sales exclusively through its mail order catalog to expansion into retail storefronts throughout the US. Unable to execute a new strategy within its existing business model, Sears developed new structures and adapted old structures to a new retail business strategy. This necessitated adjustment of management responsibilities, "a redefinition of the lines of authority and communication, and the development of new types of information to flow through these lines." Chandler notes the transition undertaken by Sears proceeded very slowly—from 1929 to 1948—and suffered from implementation of "an incorrect plan with wrong objectives" and initial hesitance to develop new structures, instead of reliance on existing structures, to execute the new strategy.[20] Sears's leadership eventually recognized this

[18] Chandler, *Strategy and Structure*, 13-14.
[19] Chandler, *Strategy and Structure*, 55-56.
[20] Chandler, *Strategy and Structure*, 225-226.

problem and, through trial and error, created new structures suitable to manage the incredible growth generated by its shift in strategy.

Based on his analysis of DuPont and Sears (as well as General Motors and Standard Oil), Chandler's thesis is that "structure follows strategy" in explaining how "different organizational forms result from different types of [industrial enterprise] growth." Chandler further concludes that "a company's strategy in time determined its structure."[21] Admittedly, Chandler tailored his notions of strategy and structure to suit a comparative analysis of US business administration for major corporations and industries. For present purposes, his definitions also prompt valuable questions and offer useful measures for analysis of the US government's decentralized enterprise against transnational crime and associated information sharing efforts.

This study seeks to determine if structure follows strategy accurately in creating institutions and processes for effective information sharing on transnational organized crime. Chandler's definition of strategy provides useful measures with which to analyze and assess US strategy documents. First, do these documents state the "basic long-term goals and objectives" of the "enterprise" against transnational organized crime, and information sharing efforts within it, in a clear, consistent manner? Second, are the selected "courses of action and the allocation of resources" appropriate to confront the threat and share information effectively? In accordance with Chandler's definition of structure, the measure is whether institutions and processes involved in sharing information on transnational organized crime are crafted with clear "lines of authority and communication" to enable an effective "flow" of "information and data." Chandler's interrelated notions of strategy and structure provide important tools for the analytical framework of this study. Schein's ideas on organizational culture complement Chandler's ideas and serve to bind strategy and structure even closer together; moreover, Schein's thinking on organizational culture explains complex human interactions and the critical role of leadership, areas for which strategy and structure may not fully account.

Schein's *Organizational Culture*

Proper leadership translates strategy into action through engagement of useful structures. Effective leaders develop and refine an organization's culture to motivate

[21] Chandler, *Strategy and Structure*, 13-14, 383.

personnel continuously to pursue strategic goals and to enhance organizational structures for optimal pursuit of strategic goals. This study borrows Edgar Schein's ideas on organizational culture to assess whether relevant US government strategies and structures promote an effective information sharing culture to fight transnational organized crime.

In his influential management textbook, Schein establishes a relationship between culture and leadership and explores the connection between the two concepts. He defines culture and provides a model with which to analyze culture and leadership's role in its creation and evolution. Schein leverages his extensive corporate consulting background to provide numerous examples that illuminate concepts and support his relationship model for organizational culture and leadership. Overall, Schein's fundamental argument is "(1) that leaders as entrepreneurs are the main architects of culture, (2) that after cultures are formed, they influence what kind of leadership is possible, and (3) that if elements of the culture become dysfunctional, leadership can and must do something to speed up cultural change."[22]

Schein defines organizational culture as "a pattern of shared basic assumptions learned by a group as it solved its problems of external adaptation and internal integration, which has worked well enough to be considered valid and, therefore, to be taught to new members as the correct way to perceive, think, and feel in relation to those problems." Schein asserts that "the most fundamental characteristic of culture is that it is a product of social *learning*" (emphasis in original). Active leadership shapes and guides group learning integral to culture; therefore, Schein describes the "fundamentally intertwined" relationship between culture and leadership as "two sides of the same coin."[23] For example, Schein recounts the emotional, highly competitive, individual-centric, anarchic environment among Digital Equipment Corporation (DEC) employees to demonstrate how a company's founder/leader establishes an organizational culture and reinforces it through subsequent decisions and actions. The initial culture established by DEC's founder proved profitable and successful, and the company thrived for decades.

[22] Edgar H. Schein, *Organizational Culture and Leadership*, 4th ed. (San Francisco: Jossey-Bass, 2010), xi, xiii.
[23] Schein, *Organizational Culture and Leadership*, xi, 17-18, 22.

Unfortunately, as the computer industry evolved, DEC's leadership and cultural stagnation translated into less attractive products, resulting in the sale of the company.[24]

To explain his culture and leadership model, Schein first identifies categories of culture, including macrocultures, microcultures, subcultures, and organizational cultures. The latter includes private, public, non-profit, and government organizations. Schein then identifies levels of culture: *artifacts* are "visible and feelable structures and processes" and "observed behavior"; *espoused beliefs and values* include "ideals, goals, values, aspirations," and "ideologies and rationalizations"; and *basic underlying assumptions* are "unconscious, taken-for-granted beliefs and values."[25] It is useful for understanding this study's analytical framework to explore these levels in more detail.

Artifacts include things accessible through one's senses (e.g., language, mannerisms, clothing, art, technology and products). The key to identification of an artifact is its observability to an outsider. For instance, popular fast-food restaurants engage multiple senses through a variety of artifacts to ensure customers know exactly where they are and remember their restaurant experience (e.g., trademarks, product names and packaging, employee uniforms, building architecture, customer service language). However, Schein cautions that an artifact is "both easy to observe and very difficult to decipher." Schein cites ancient Egyptian and Mayan pyramids as examples where similar geometric constructions provide visible representations of civilizational strength, yet the meaning of the pyramids in each culture is invisibly different: "tombs in one, temples as well as tombs in the other."[26] The idea is that the ability to sense something does not guarantee a precise or even correct appreciation of its meaning. Further investigation is required to ascertain meaning, leading to the next level of culture.

Espoused beliefs and values include the stated rationale or purpose for the existence of an organization, and expectations of desired performance for the organization at large and individual members. Schein notes that preferred and actual behavior may be incongruous, causing anxiety within an organization struggling to establish or conform to a culture. Schein provides the example of the "The HP Way"

---

[24] Schein, *Organizational Culture and Leadership*, 9, 35-44. According to Schein, DEC was founded in the mid-1950s and sold to Compaq Corporation in 1996.
[25] Schein, *Organizational Culture and Leadership*, 2, 24.
[26] Schein, *Organizational Culture and Leadership*, 23-24.

where Hewlett-Packard promoted "consensus management and teamwork" but computer engineers felt compelled to compete with each other and to engage in political maneuvers.[27] Like artifacts, espoused beliefs and values provide significant cultural cues, yet a fuller appreciation of an organization's culture may elude an observer due to contradictions between ideals and practice. True meaning lies at the next level of culture.

To gain a rich understanding of an organizational culture—"to decipher the pattern, and to predict future behavior correctly"—requires determination of basic underlying assumptions. For Schein, "implicit, unconscious assumptions … often deal with fundamental aspects of life": truth, time and space, human nature, proper human relations, work-family balance, gender roles, etc.[28] For example, Schein compares the underlying assumptions for a corporate "family" between DEC and Ciba-Geigy, a Swiss pharmaceutical company. In the DEC family, co-equal members fought fiercely but loved each other and valued family loyalty. At Ciba-Geigy, a parent-child relationship existed where employees behaved in accordance with company rules and obeyed corporate leadership, who, in turn, supported and took care of employees.[29] In essence, organizational culture contains the basic assumptions under which an organization operates, as reflected in behaviors and attitudes toward both internal and external audiences. Basic assumptions are fundamental to organizational culture, as these "taken-for-granted" beliefs underpin the culture. They are taken for granted because a leader, or group of leaders, has demonstrated the effectiveness of a certain way of thinking or acting that the organization as a whole views as likely to continue to succeed. When assumptions are challenged or proven faulty, it is the responsibility of culturally-savvy leaders to guide an organization through cultural change to eliminate or reduce anxiety and create an effective operating environment.[30]

This study leverages Schein's organizational culture model to analyze strategies and structures in place to promote information sharing on transnational organized crime.

---

[27] Schein, *Organizational Culture and Leadership*, 27.
[28] Schein, *Organizational Culture and Leadership*, 27, 31-32.
[29] Schein, *Organizational Culture and Leadership*, 52. According to Schein, Ciba-Geigy merged with another company in recent years to form Novartis International. See Schein, *Organizational Culture and Leadership*, 10.
[30] Schein, *Organizational Culture and Leadership*, 33.

Specifically, this study analyzes the performance of specific institutions and processes in US government organizations, which reflects the effectiveness, or lack thereof, of leaders in shaping positive cultural environments for effective information sharing. Additionally, this study discusses analogous counterterrorism efforts to determine if organizational cultural learning from counterterrorism information sharing efforts may allow leaders to drive information sharing for transnational organized crime to build upon lessons learned by federal agencies, including DOD, since the 9/11 attacks.

Theoretically, solutions to information sharing problems with transnational organized crime lie in ensuring the presence of sound strategy, effective structures to implement the strategy, and organizational cultures that embrace and adapt to the strategy and leverage structural resources fully to achieve strategic goals. Where these elements appear to be lacking or missing is most likely where the need for improvement exists, and identification of problems is the first step toward improvement. The next chapter begins the process of problem identification with analysis of key US strategy documents on transnational organized crime and information sharing.

Chapter 3

Analysis of Key US Strategy Documents

This chapter analyzes specific US strategy documents for transnational organized crime and information sharing, including the 2010 *National Security Strategy*, 2011 *Strategy to Combat Transnational Organized Crime*, 2011 *National Military Strategy*, 2011 *DOD Counternarcotics & Global Threats Strategy*, 2012 *National Strategy for Information Sharing and Safeguarding*, 2007 *DOD Information Sharing Strategy*, and 2010 *DOD Information Enterprise Strategic Plan*.[1] Collectively, relevant strategies should provide clear direction, useful guidance, and prioritization of effort for the DOD toward a shared goal to improve information sharing on transnational organized crime. This analysis inquires if this is the case and seeks to identify guidance issues that cause problems in policy implementation and execution.

As described in the previous chapter, Chandler's notions of *strategy* and *structure* and Schein's *organizational culture* provide a composite theoretical framework with which to analyze selected strategy documents. This chapter focuses on the strategy and culture elements of the framework. First, this study applies Chandler's definition of strategy against key US strategy documents to assess whether they state (1) "basic long-term goals and objectives" of the "enterprise" for sharing information on transnational organized crime in a clear, consistent manner, and whether (2) selected "courses of action and the allocation of resources" appear appropriate to share threat information effectively. Next, Schein's organizational culture model offers the ability to discern any espoused beliefs and values or basic underlying assumptions that relevant strategy documents seek to promote. Moreover, Schein's model provides a lens to view organizational culture change encouraged by these strategy documents.

Strategy and Culture: Transnational Organized Crime

***National Security Strategy*.** In its 2010 *National Security Strategy* (*NSS*) document, the Obama Administration identifies transnational organized crime as a

[1] The White House released an updated *National Security Strategy* in February 2015. The author did not include analysis of this strategy document due to time constraints for thesis production.

significant threat to national security. Transnational criminal organizations "foment insecurity abroad and bring people and goods across our own borders that threaten our people."[2] Transnational criminal organizations pose a physical threat to the safety of American citizens at home and abroad through illicit trafficking and, at times, mutually beneficial interaction with terrorist organizations. Transnational organized crime, including cyber crime, undermines and corrupts legitimate government and financial institutions. Transnational criminal organizations weaken partner states to the US and contribute to regional instability.[3] Mindful of this general review of transnational organized crime, it is important to step back and orient this threat within the broader interest framework of the *NSS* in order to understand derivative goals and objectives for the effort against transnational organized crime found in supporting strategy documents.

The *NSS* advances "four enduring national interests"—or goals to use Chandler's term—labeled as security, prosperity, values, and international order.[4] Efforts against transnational organized crime fall under international order. According to President Barack Obama, "The expanding size, scope, and influence of transnational organized crime and its impact on U.S. and international security and governance represent one of the most significant of those [global] challenges" to the current international order.[5] In short, the Obama Administration views and confronts transnational organized crime as a threat to a continuing US-led international order that serves the security, prosperity, and values of American citizens and allied/partner nations.

To combat this threat, the *NSS* articulates the need for a "multidimensional strategy that safeguards citizens, breaks the financial strength of criminal and terrorist networks, disrupts illicit trafficking networks, defeats transnational criminal organizations, fights government corruption, strengthens the rule of law, bolsters judicial systems, and improves transparency."[6] As with other national security threats and challenges, the Obama Administration envisions a "whole of government" approach to

---

[2] *The National Security Strategy of the United States of America* (Washington: The White House, May 2010), 8, 49.
[3] *National Security Strategy*, 49.
[4] *National Security Strategy*, 7, 17.
[5] *Strategy to Combat Transnational Organized Crime*, cover letter by President Barack Obama.
[6] *National Security Strategy*, 49.

achieve this diverse, complex set of objectives against transnational organized crime. The Administration strives to "balance and integrate all of the tools of American power"—defense, diplomacy, economic, development, homeland security, intelligence, strategic communications, and "the American people and the private sector"—in its efforts to counter transnational organized crime.[7]

For the second aspect of Chandler's notion of strategy, the *NSS* offers no specific courses of action or allocation of resources to tackle the transnational organized crime problem. However, the Obama Administration insists on specific steps for counterterrorism efforts that appear analogous and helpful for information sharing on transnational organized crime. To prevent terrorist attacks within the US, the Administration expects the full engagement of existing US capabilities and cooperation among homeland security, law enforcement, and intelligence agencies. To augment federal capabilities, the White House intends to "continue to integrate and leverage state and major urban area fusion centers that have the capability to share classified information."[8] In this way, fusion centers provide a multiplication of force to collect, analyze, and disseminate timely information on terrorist threats, especially when enabled to handle classified data. Next, the Administration proposes to "establish a nationwide framework for reporting suspicious activity."[9] As with fusion centers, the intent is to create a system that acts as a force multiplier through expanding the pool of individuals and agencies able to report information or incidents that may appear insignificant individually, but cumulatively provide an intelligence picture of a potential threat requiring counteraction. Importantly for this study, the Obama Administration seeks to "implement an integrated approach to our counterterrorism information systems to ensure that the analysts, agents, and officers who protect us have access to all relevant intelligence throughout the government."[10] This step represents an acknowledgement of the need to continue to improve information sharing capabilities, a critical work in

[7] *National Security Strategy*, 14-16. The 2010 *National Security Strategy* also encourages a "collective strategy with other nations facing the same threats," the relevance of which is outside the scope of this study. See *National Security Strategy*, 49.
[8] *National Security Strategy*, 20.
[9] *National Security Strategy*, 20.
[10] *National Security Strategy*, 20.

progress encouraged fervently in *The 9/11 Commission Report* of 2004. While directed at the fight against terrorism in the homeland, these steps also hold great promise for information sharing efforts to combat a related threat—transnational organized crime.

Though non-specific to transnational organized crime, the *NSS* acknowledges the continuing need for improvements in inter-departmental and inter-agency cooperation. The Obama Administration identifies several ways to enhance cooperation, including resource alignment in accordance with its strategy guidance, personnel education and training (presumably including emphasis on cooperation), and enforcement of existing cooperation requirements.[11] Recognition of an enduring need to improve cooperation at the federal level and throughout all levels of government reflects a continual effort to remedy cooperation shortfalls identified as a major contributor to the failure to prevent the 9/11 attacks.[12] It also highlights the tension between separation of powers and federalism in the US governance system and the need for those separated powers and levels of government to cooperate to the fullest extent allowed within the bounds of distinct authorities and jurisdictions to combat national security threats most effectively.

As a foundational policy document, the *NSS* contains numerous references to cultural values that undergird pursuit of US national interests. In fact, the four enduring national interests—security, prosperity, values, and international order—are goals of the strategy, but they also represent espoused cultural beliefs and values, to use Schein's terms. The Strategy promotes fundamental American beliefs and values, including democracy, the rule of law, respect for human rights, civil liberties and privacy protections, and government transparency. In the context of development, the Strategy supports values and beliefs in national stability, institutional integrity, citizen security, the integrity and unimpeded function of financial and commercial markets and cyberspace, and the development of struggling, failing, or failed states.[13] These values and beliefs represent separate ingredients of a possible antidote for the scourge of transnational organized crime. Overall, to support espoused beliefs and values, the US must remain secure and must lead in order to defend itself, allies and partners, and a stable, valuable

[11] *National Security Strategy*, 14.
[12] *The 9/11 Commission Report*, 403, 418.
[13] *National Security Strategy*, 5, 15, 35-37.

international order. These basic underlying assumptions surface throughout the Strategy.

The *NSS* promotes organizational culture change through advocacy of a whole-of-government approach. To operationalize and make this effective, organizational leaders throughout the US government must encourage and foster a culture of inter-agency cooperation instead of competition. Moreover, the approach pushes executive branch entities to recognize the value of partnerships with state and local authorities, international governments, and industry representatives. Overall, the Strategy envisions "a comprehensive range of national actions" to safeguard US interests within "a broad conception of what constitutes our national security."[14] This vision includes transnational organized crime; therefore, a separate US strategy document provides more specific guidance on efforts to combat this stated national security threat.

***Strategy to Combat Transnational Organized Crime*.** The significant—albeit brief—discussion of transnational organized crime in the *NSS* established a foundation for a more specific national strategy document to update and broaden the law enforcement-centric 2008 *Law Enforcement Strategy to Combat International Organized Crime*. In July 2011, the White House published a *Strategy to Combat Transnational Organized Crime*. This document expands upon discussion of transnational organized crime threats identified in the *NSS*, including concern that transnational criminal organizations corrupt and ally with elements of foreign governments to enhance criminal activities, while offering some governments opportunities to leverage transnational criminal organizational capabilities to harm US national security interests. To reflect increased concern over "converging threats" based on a "crime-terror-insurgency nexus," the Obama Administration uses the term "transnational organized crime" to convey the complexity of a phenomenon considered not only a problem for law enforcement, but a national security threat worthy of attention from all instruments of US national power.[15]

This specific strategy advocates a "whole-of-government" approach—as in the *NSS*—to achieve specific objectives toward a desired "end-state," or goal: to reduce transnational organized crime to a "manageable public safety problem."[16] The whole-of-

[14] *National Security Strategy*, 14, 51.
[15] *Strategy to Combat Transnational Organized Crime*, 3, 6.
[16] *Strategy to Combat Transnational Organized Crime*, 1, 4.

government approach finds expression in a "single unifying principle: *to build, balance, and integrate the tools of American power to combat transnational organized crime and related threats to national security—and to urge our foreign partners to do the same*" (emphasis in original).[17] The Obama Administration also offers an "integrated and comprehensive approach" designed "to *raise international awareness* about the reality of the TOC [transnational organized crime] threat to international security; *galvanize* multilateral action to *constrain* the reach and influence of TOC; *deprive* TOC of its enabling means and infrastructure; *shrink* the threat TOC poses to citizen safety, national security, and governance; and *ultimately defeat* the TOC networks that pose the greatest threat to national security" (emphasis in original).[18] To achieve the end-state and set the desired conditions of the integrated and comprehensive approach, the US government pursues several objectives consistent with the *NSS*. Within one of the objectives, the White House specifies the need for "information sharing at home with State and local agencies," an important general reference to similar steps the *NSS* promotes for counterterrorism.[19]

Two critiques regarding the approach and end-state sought in the plan are in order. First, in both the *NSS* and *Strategy to Combat Transnational Organized Crime*, the White House advocates a whole-of-government approach. Specifically, the *NSS* offers a "multidimensional strategy" while the *Strategy to Combat Transnational Organized Crime* seeks an "integrated and comprehensive approach" to confront transnational organized crime. Do they align consistently? Apparently, the Obama Administration believes so; a direct quote of the multidimensional strategy from the *NSS* appears in the introduction chapter of the *Strategy to Combat Transnational Organized Crime*, which implies the articulated requirement for a multidimensional strategy against transnational organized crime prompted the 2011 strategy document and its integrated and comprehensive approach.[20] The desired conditions and five objectives of the integrated and comprehensive approach in the *Strategy to Combat Transnational Organized Crime* appear to align with the objectives of the multidimensional strategy of the *NSS*.

---

[17] *Strategy to Combat Transnational Organized Crime*, 1, 4.
[18] *Strategy to Combat Transnational Organized Crime*, 13.
[19] *Strategy to Combat Transnational Organized Crime*, 13-14; *National Security Strategy*, 20.
[20] *Strategy to Combat Transnational Organized Crime*, 3.

However, the Administration can be faulted for introducing a slight bit of confusion with its approach-within-an-approach language in the *Strategy to Combat Transnational Organized Crime*. Perhaps a distinction without a difference, it may have been more helpful for executive agencies to grapple only with understanding one term for the approach taken (whole-of-government) instead of two terms (whole-of-government and integrated and comprehensive approach).

Second, the *Strategy to Combat Transnational Organized Crime* seeks an end-state that reduces transnational organized crime to a "manageable public safety problem."[21] In essence, the White House elevates transnational organized crime in importance by deeming it a national security threat but, through its strategy, strives to return the phenomenon to a law enforcement concern. Does this goal make sense for the perceived "converging threat" of transnational organized crime, insurgency, and terrorism? Law enforcement agencies traditionally handle organized crime investigations, and law enforcement plays a large role in the detection, prevention, or reaction to terrorist acts. On the other hand, insurgencies involve an armed confrontation between state and non-state actors where law and order has broken down and law enforcement is at best a secondary struggle. It is possible to defeat an insurgent group through use of military force, pacification programs, negotiation, etc. (e.g., Great Britain in Malaya, Peru against the Shining Path). Audrey Kurth Cronin argues persuasively that it is also possible in various ways to "win" against terrorist organizations and "return the threat [of terrorism] to a manageable nuisance."[22] Even if organized crime and terrorism can arguably be reduced to manageable public safety problems, an insurgency cannot and should not be handled solely as a law enforcement matter. Governments strive to defeat, not manage, insurgencies. In recent decades, insurgent and terrorist groups increasingly resorted to criminal activities to fund their activities due to loss of state sponsorship and difficulties in funding from "legitimate" donors. When insurgent or terrorist groups arise and fund activities through criminal means, as is highly likely to continue to occur, will the US and other nations seek to "manage" or "defeat" this converging threat?

---

[21] *Strategy to Combat Transnational Organized Crime*, 1, 4.
[22] Audrey Kurth Cronin, *How Terrorism Ends: Understanding the Decline and Demise of Terrorist Campaigns* (Princeton: Princeton University Press, 2009), 197.

The point of this particular critique is that the end-state may be unrealistic and therefore counterproductive for national security professionals charged with confronting transnational organized crime alone, or in conjunction with insurgent or terrorist groups, with all available ways and means. In terms of Chandler's notion of strategy, an unrealistic end-state or goal in strategy increases the difficulty in crafting a matching structure, essentially leading plans for an enterprise astray from the beginning. For Schein's organizational culture, an unrealistic end-state breeds disillusionment within an organization, reducing "buy-in" and weakening organizational unity.

The *Strategy to Combat Transnational Organized Crime* is quite specific with respect to courses of action but less so for allocation of resources. Overall, the Obama Administration directs "56 priority actions" for the US government to undertake against transnational organized crime, focused primarily on measures in the homeland to decrease domestic effects of the threat (e.g., disrupt illicit traffic flows, dismantle networks operating in the US, reduce drug demand).[23] Of note, the first section of "other priority actions" discusses how to "enhance intelligence and information sharing."[24] To remedy perceived intelligence gaps for transnational organized crime due to its lower priority relative to counterterrorism and to account for growth and complexity in the threat since the late 1990s, the Administration seeks to improve a variety of intelligence capabilities (i.e., signals, human, and open source) on transnational organized crime.[25]

For intelligence and information sharing enhancement, the Obama Administration provides priorities and priority actions (terms similar to Chandler's courses of action). These priorities and priority actions encourage various new processes using existing and new institutions across the federal government—including the DOD—and among other levels of government in the US to improve information sharing on transnational organized crime. Specifically, the Strategy pushes existing and new fusion centers toward further collaboration, promotes cooperation across law enforcement, homeland

[23] *Strategy to Combat Transnational Organized Crime*, cover letter by President Obama, 4, 16.
[24] *Strategy to Combat Transnational Organized Crime*, 4, 17. To provide a simple metric of its relative importance, the 2011 *Strategy to Combat Transnational Organized Crime* devotes 3 of its 33 pages to discuss intelligence and information sharing for transnational organized crime (including a two-page inset box on key information sharing institutions), with references to the importance of intelligence and information sharing interspersed throughout the document.
[25] *Strategy to Combat Transnational Organized Crime*, 17.

security, intelligence, military, and other relevant disciplines, and supports relationship-building among authorities at all US governance levels with a stake in confronting the threat. Overall, the Strategy represents a thoughtful effort in the right direction to motivate federal cooperation on transnational organized crime and information sharing.

For allocation of resources, the Strategy postures the US government "to combat TOC networks that pose a strategic threat to Americans and to U.S. interests in key regions."[26] Notably, the Obama Administration views transnational organized crime and drug trafficking "as increasingly intertwined," which removes a traditional law enforcement obstacle where organized crime and drug trafficking (and gangs) receive separate treatment by agencies resourced differently; the intent is synergistic efforts that "maximize the impact of U.S. resources" on transnational criminal organizations and involved actors.[27] The Administration charges the Interagency Policy Committee (IPC) on Illicit Drugs and Transnational Criminal Threats, a combined National Security Staff and Office of National Drug Control Policy entity, with implementation of the Strategy using a whole-of-government approach. To further emphasize that transnational organized crime represents more than a law enforcement problem, the Strategy establishes an "interagency Threat Mitigation Working Group" to coordinate use of all necessary US instruments of power against designated high-threat transnational criminal organizations.[28] While the IPC and Threat Mitigation Working Group represent novel resource allocations against transnational organized crime, the White House relies heavily on existing institutional resources distributed throughout the executive branch to confront this threat in accordance with strategy guidance.

The *Strategy to Combat Transnational Organized Crime* is more than a strategy; it is a hybrid strategy-implementation plan document. Specific strategy documents for information sharing split between overarching strategy documents and separate implementation plans. This is not the case for transnational organized crime. The *Strategy to Combat Transnational Organized Crime* contains strategy and planning elements, including a single unifying principle, an end-state, approaches, objectives,

[26] *Strategy to Combat Transnational Organized Crime*, 5.
[27] *Strategy to Combat Transnational Organized Crime*, 4.
[28] *Strategy to Combat Transnational Organized Crime*, 4, 13.

priorities, and priority actions. Each use of these terms appears sensible in the context of a hybrid strategy-implementation plan document; however, there is ample room for confusion in the diversity of terms. For example, what is the difference between the single unifying principle and a whole-of-government (or integrated and comprehensive) approach when each advocates combined use of all US instruments of power against transnational organized crime? For enhancement of information sharing on transnational organized crime, the Obama Administration provides numerous priorities and 56 priority actions, yet they are essentially interchangeable, meaning priorities could have been listed under priority actions or vice-versa. Overall, the Strategy is not difficult to read and understand, but it nevertheless suffers somewhat from a lack of clarity in terminology usage that invites confusion for organizations tasked to implement the Strategy.

As a supplement to the *NSS*, it is not surprising the *Strategy to Combat Transnational Organized Crime* reflects the same cultural values. Expanding upon the espoused beliefs and values, basic underlying assumptions, and organizational culture change promoted in the *NSS*, the Obama Administration re-emphasizes the importance of information and intelligence to counter threats, specifically in the context of transnational organized crime.[29] This basic underlying assumption supports pursuit of enhanced capabilities and processes to collect and process information and convert it into useful shared intelligence that empowers relevant authorities to make the best decisions to confront transnational organized crime. The Strategy assumes information sharing is an optimal way to foster collaborative efforts within US government agencies, among all levels of government in the US, and with international partners to combat the threat—and promotes this mindset change throughout all aspects of the transnational organized crime strategy. This accords with Chandler's notion of strategy; in this case, strategy provides direction and focus in its promotion of information sharing, which will drive matching structural and cultural adjustments.

National Military Strategy. In the 2011 *National Military Strategy (NMS)*, the Chairman of the Joint Chiefs of Staff (CJCS) identifies transnational criminal organizations as non-state actors that "undermine the rule of law, perpetuate and

[29] *Strategy to Combat Transnational Organized Crime*, 4, 17.

accelerate violence in the international system, and challenge states' ability to respond."[30] As in the *NSS* and *Strategy to Combat Transnational Organized Crime*, the *NMS* cites "a nexus of interests" among transnational criminal organizations and terrorist groups who exploit the "global commons" (sea, air, and space) and "globally connected domains" (cyberspace).[31] Since "joint assured access to the global commons and cyberspace constitutes a core aspect of U.S. national security and remains an enduring mission for the Joint Force," threats to these global interests necessitate action.[32]

The US military recognizes the national security threat posed by transnational criminal organizations and accounts for this threat within defined US national interests, overarching military objectives and existing military authorities. In line with the enduring national interests (i.e., goals) from the *NSS*, the *NMS* identifies four "national military objectives": "Counter Violent Extremism, Deter and Defeat Aggression, Strengthen International and Regional Security, and Shape the Future Force."[33] US military efforts against transnational organized crime fit within the objectives to strengthen international and regional security and counter violent extremism—when a nexus exists between transnational organized crime and a terrorist or insurgent group.

The CJCS states the US military stands ready to confront "transnational security challenges" in a cooperative, combined manner working with other US instruments of power—diplomacy, development, etc.— and foreign partners. While the *NSS* and *Strategy to Combat Transnational Organized Crime* both promote a whole-of-government approach, the *NMS* supports "whole-of-nation approaches" to address national security threats and challenges, including transnational organized crime.[34] The CJCS does not explain the rationale for the different choice in terminology or provide a precise meaning for "whole-of-nation," but implies the approach goes beyond the capabilities of US instruments of power to include those of partner nations. Within US capabilities, the Strategy advocates for "authorities for a pooled-resources approach to

[30] *The National Military Strategy of the United States of America* (Washington: The Chairman of the Joint Chiefs of Staff, February 2011), 4.
[31] *National Military Strategy*, 3.
[32] *National Military Strategy*, 9.
[33] *National Military Strategy*, 4.
[34] *National Military Strategy*, 6, 8, 9, 15-16, 21.

facilitate more complementary efforts across departments and programs, integrating defense, diplomacy, development, law enforcement, and intelligence capacity-building activities." The CJCS identifies this requirement within the context of security assistance programs for foreign partners, but the need applies equally to efforts against transnational organized crime, including improvement of information sharing across various US departments and agencies. The Strategy encourages cooperation with the Department of Homeland Security, including the US Coast Guard, "to improve air, maritime, space, cyberspace and land domain awareness to help secure the approaches to our continent and Nation."[35] Improving awareness and securing approaches allude, if only indirectly and not solely, to respective needs to enhance information sharing and counter the transit of trafficked goods by transnational criminal organizations.

The *NMS* does not provide specific courses of action or an allocation of resources to confront transnational organized crime; instead, it directs geographic combatant commanders to "tailor [planning] to their region and coordinate across regional seams" in accordance with the whole-of-nation approach, which presumably includes planning and resources to counter transnational organized crime. The Strategy also reinforces support for funding and training of National Guard assets to support homeland defense and defense support of civil authorities, which should include efforts against transnational organized crime and requisite information sharing.[36]

The three themes of the *NMS* provide insights into how the CJCS promotes cultural change within the US military to improve effectiveness, which has implications for information sharing efforts against transnational organized crime. The first theme is that leadership is the key variable in attacking "complex security challenges," since "the Joint Force's leadership approach is often as important as the military capabilities we provide." The CJCS insists, "Our focus on leadership, not simply power, necessitates that we emphasize our values and our people as much as our platforms and capabilities."[37] The emphasis on leadership represents an espoused belief and value but also reflects a basic underlying assumption within US military service cultures that

[35] *National Military Strategy*, 10, 15-16.
[36] *National Military Strategy*, 11, 15.
[37] *National Military Strategy*, cover letter by Admiral Michael G. Mullen, CJCS, 16.

effective leadership is the key to mission success. It also supports an espoused belief and value and basic underlying assumption in the *NSS* that the US should not only provide an example for other nations to imitate, but an example of leadership for others to follow.[38]

While the theme of leadership permeates the *NMS*, two other themes also appear repeatedly: the need to "deepen" relationships with allies and create relationships with new partners to cope with a "changing security environment," and preparation for "an increasingly dynamic and uncertain future in which a full spectrum of military capabilities and attributes will be required" to deter and defeat enemies. The theme of deepening security relationships aligns with a whole-of-nation approach, which is an espoused belief in the power of "concerted" efforts by various US entities and foreign partners to confront threats that challenge a beneficial, stable, US-led international order.[39] The need for full-spectrum military capabilities reflects a basic underlying assumption—based on the frequency and diversity of conflicts and operations in recent decades—that the US military will continue to be employed against a variety of hostile actors with a wide range of capabilities and intentions. Moreover, this is a reminder for the values of flexibility in resource use and agility in thinking, especially pertinent for the US military in grappling with defining its role against transnational organized crime. To return to the leadership theme, the need for full-spectrum military capabilities exposes a potential tension where confrontation against a threat—such as a transnational criminal organization—requires various military capabilities but does not require or allow (due to lack of legal authorities) military leadership against the threat.

If transnational organized crime is, at a minimum, a predominant regional threat, why does it receive so little attention in the *NMS* (or the 2014 *Quadrennial Defense Review*)? Additionally, a 2012 defense strategic guidance document makes *no* direct, specific mention of transnational organized crime or transnational threats, though it recognizes the threat posed by non-state actors to the global commons.[40] The White House designates transnational organized crime as a significant national security threat with a dedicated strategy document, yet top military strategy documents discuss it

---

[38] *National Security Strategy*, 1, 7, 10, 17, 36-37, 51.
[39] *National Military Strategy*, cover letter by Admiral Michael G. Mullen, CJCS, 5-7.
[40] *Sustaining Global Leadership: Priorities for 21st Century Defense* (Washington: Secretary of Defense, January 2012), 3.

infrequently compared to, as examples, climate change and energy efficiency. The US military should take steps to minimize its environmental impact and should consume energy more efficiently, but the fundamental role of the US military is to deter and defeat threats—real-time threats posed by flesh-and-blood human actors. Arguably, this represents a priority disconnect among strategy documents—or to use Schein's terminology, espoused beliefs and values—even before actions expose contradictions in espoused beliefs and values. To be fair, the answer may lie more with DOD's basic underlying assumption that it serves a supporting function in efforts against transnational organized crime. However, this does not provide a wholly satisfactory answer since the *NMS* advocates for expanded military authorities to confront threats more effectively—including transnational organized crime—in a whole-of-nation approach, and the *DOD Counternarcotics & Global Threats Strategy* also advises broadened authorities may be necessary for the US military to better combat transnational organized crime.[41]

DOD Counternarcotics & Global Threats Strategy. In 2011, the Deputy Assistant Secretary of Defense (DASD) for Counternarcotics & Global Threats published the *DOD Counternarcotics & Global Threats Strategy*, which describes transnational organized crime as a "significant, multilayered, and asymmetric threat to our national security." The Strategy limits its scope to trafficking in commodities—"drugs, small arms and explosives, precursor chemicals, and illicitly-gained and laundered money"—across international borders, and omits weapons of mass destruction, counterfeit products, and human trafficking. DASD cites the crime-terror-insurgency nexus as a "commonly recognized national security threat" and asserts illicit traffickers present "all the hallmarks of a threat to U.S. national security."[42] To engage this threat, DOD exercises authorities granted to conduct drug interdiction and counterdrug activities, primarily in support of other federal entities and allied/partner nations. DOD operations against trafficking in small arms and explosives, precursor chemicals, and laundered money must be "reasonably related to its counterdrug and counterterrorism efforts," a

[41] *National Military Strategy*, 15-16; *DOD Counternarcotics & Global Threats Strategy*, 21, which states, "DOD authorities may require supplementation or amendment" to confront the dynamic threat of transnational organized crime.
[42] *DOD Counternarcotics & Global Threats Strategy*, 4-5.

determination made on a case-by-case basis.[43] The intent is to posture DOD vis-à-vis transnational organized crime (at least a portion of it) and explain "how DOD can rapidly deploy resources in support of U.S. and partner law enforcement organizations to disrupt and degrade an ever-changing and adaptive threat."[44] In this way, DOD strategy supports the multidimensional strategy and whole-of-government approach of the *NSS*.[45]

The overall goal for DOD efforts against transnational organized crime is "to limit substantially and sustainably the impact of illegal drugs and other illicit trafficking organizations or networks" against the US. To achieve this goal, one of the "four guiding tenets" for the DOD is "to promote higher-performing interagency networks to galvanize productivity and deliver results," which implies promotion of information sharing.[46] The *DOD Counternarcotics & Global Threats Strategy* contains strategic goals with corresponding objectives. Of interest for this study is the third strategic goal:

> The size, scope, and influence of targeted TCOs [transnational criminal organizations] and trafficking networks are mitigated such that these groups pose only limited, isolated threats to U.S. national security and international security. The United States and partner nations have developed layered, coordinated approaches that regularly disrupt the operations of these organizations and networks, limit their access to funding, reduce their assets, and raise their costs of doing business.[47]

The development of "layered, coordinated approaches" implies a requirement for an effective level of information sharing. Additionally, this goal contains global objectives that include seeking to "enhance or develop cooperative mechanisms with law enforcement agencies," a further allusion to the need to improve information sharing.[48]

For courses of action, the Strategy states explicitly that it "does not include specific actions and activities." Instead, DASD seeks to inject consideration of transnational organized crime threats into the strategy and planning development cycle throughout DOD—including "functional and regional sub-strategies" and Combatant Command Theater Campaign Plans—and other relevant executive branch agencies. To

[43] *DOD Counternarcotics & Global Threats Strategy*, 4-5.
[44] *DOD Counternarcotics & Global Threats Strategy*, 6.
[45] *DOD Counternarcotics & Global Threats Strategy*, 7, 17.
[46] *DOD Counternarcotics & Global Threats Strategy*, 8, 11.
[47] *DOD Counternarcotics & Global Threats Strategy*, 13-14.
[48] *DOD Counternarcotics & Global Threats Strategy*, 16.

approve allocation of resources, DASD reviews sub-strategies and plans to determine if requests for funding align with "at least one strategic goal or objective" in the Strategy.[49] In contrast to the *Strategy to Combat Transnational Organized Crime*, the *DOD Counternarcotics & Global Threats Strategy* is a pure strategy document with no specific implementation plan language. DASD leaves specific planning to operational commands and relies on them to submit timely resource requests as needed.

The *DOD Counternarcotics & Global Threats Strategy* exhibits the power of basic underlying assumptions and espoused beliefs and values in shaping the direction of the Strategy. As in other departmental documents, the Strategy states DOD's mission "is to provide the military forces needed to deter war and to protect the security of our country."[50] Indeed this is a mission statement, but it also reflects a basic underlying assumption; it is taken for granted in the sense that servicemembers, their civilian leaders, and the American public know this is what the military "is about." The Strategy espouses a key belief in the evolution of the threat environment and the "imperative to adapt" to new threats.[51] The latter also represents promotion of organizational culture change, in this case to posture DOD to deal with an evolving transnational organized crime threat. More specifically, the Strategy insists DOD requires a mindset change from a view of transnational organized crime as primarily a drug issue to a view that accounts for the full range of issues transnational organized crime represents, an interesting, perhaps conflicted notion, given the limited scope of the Strategy in addressing only trafficking in commodities.[52] Nonetheless, DOD promotes layered, coordinated approaches with diverse US and foreign partners to confront the threat effectively, which demands timely, secure information sharing.

Strategy and Culture: Information Sharing

***National Strategy for Information Sharing and Safeguarding*.** In 2012, the White House published the *National Strategy for Information Sharing and Safeguarding*, which "serves as a guide for balancing collective efforts to promote responsible sharing and safeguarding in support of national security and to enhance the safety of the

[49] *DOD Counternarcotics & Global Threats Strategy*, 17.
[50] *DOD Counternarcotics & Global Threats Strategy*, 3.
[51] *DOD Counternarcotics & Global Threats Strategy*, 3.
[52] *DOD Counternarcotics & Global Threats Strategy*, 4-5.

American people." The Obama Administration designates information as a "national asset" and promotes its widest dissemination among authorized, accountable recipients to best inform decisions that seek to uphold national security. The Administration believes US "national security relies on our ability to share the right information, with the right people, at the right time." The "right people" includes authorized individuals at any level of government in the US, in the private sector, or among foreign partners. Through more effective information sharing and safeguarding, the Administration seeks to enable increased collaboration and effectiveness among law enforcement, homeland security, intelligence, defense, diplomatic, and private sector partners.[53]

The Strategy pursues several goals to build upon improvements in information sharing since 9/11. Key objectives among these goals include an increase in the use of "common processes" across agencies and among levels for information collection and use. The Administration cites the Suspicious Activity Reporting process in use by fusion centers and law enforcement entities at various levels as an example of a common process worthy of further development and emulation.[54] To illustrate how this works, imagine a law enforcement officer in a local jurisdiction receives information from a firearms store manager on an attempt to sell a large quantity of unregistered foreign-made handguns by an individual unfamiliar to the businessman who does not appear to be a licensed vendor. The local law enforcement officer enters the suspicious activity information into a database that analysts and investigators from various interested agencies can view and act upon to refute or confirm a potential crime—possibly transnational firearms trafficking.

Another important objective is promotion of information sharing agreements among agencies. The White House seeks to "streamline" agreement development through creation of a template that addresses typical agreement barriers (e.g., information restrictions based on different missions and authorities).[55] Such a template might alleviate problems with agreements between agencies of separate departments (e.g., Immigration and Customs Enforcement and FBI), for instance, in efforts to increase

[53] *National Strategy for Information Sharing and Safeguarding*, 2, 3, 14, 16.
[54] *National Strategy for Information Sharing and Safeguarding*, 8.
[55] *National Strategy for Information Sharing and Safeguarding*, 8.

information flows regarding human trafficking into the US.

The Strategy also seeks to improve the ability of authorized individuals to find and access information necessary for mission performance in databases external to their organization, which requires policy clarity and "technical guidance for implementing interoperable processes and technology."[56] For example, a US Customs and Border Protection analyst pursuing an indicator on possible counterfeit currency entries at domestic ports should be familiar with US Secret Service databases containing counterfeit currency identifiers and be able to request and retrieve pertinent information to enable appropriate decisions and actions to address potential transnational criminal activity. Additionally, databases should feed "automated capabilities" that identify "linkages across holdings and generate alerts" sent to pertinent agencies with authorities to respond.[57] In the previous example, subsequent collection of similar counterfeit currency information by the US Secret Service should trigger an alert sent to Customs and Border Protection for appropriate analytical and investigative follow-up actions.

Another key objective worth mentioning is the Obama Administration's promotion of cloud computing as a possible tool to improve information sharing, where "data centers are consolidated and computer infrastructures are employed as a shared service." Cloud computing reduces local data storage requirements and stores information in a location accessible by more users using a standard application in accordance with "identity, authentication, and authorization controls."[58] Cloud computing offers cost savings through reduced infrastructure and maintenance needs, while providing the ability to expand the availability of information to more authorized individuals. However, does this align with a "decentralized approach" to information sharing where originating agencies control and update information as necessary?[59] Granted, individual agencies can implement cloud computing internally with access granted to external agencies. Yet the temptation—with apparent encouragement by this strategy document—may be to build larger, multi-agency "clouds" in an ever-growing centralization of data storage. While a widely-accessible cloud for authorized users

[56] *National Strategy for Information Sharing and Safeguarding*, 9.
[57] *National Strategy for Information Sharing and Safeguarding*, 10.
[58] *National Strategy for Information Sharing and Safeguarding*, 9, 11.
[59] *National Strategy for Information Sharing and Safeguarding*, 10.

increases the potential for information sharing efficiency, it also poses vulnerabilities where insider threats and cyber-savvy hostile actors might benefit from increased centralization and growth in data available for exploitation in a "one-stop shop," as opposed to data stored in multiple, separate storage locations.

To mitigate this type of threat, the Obama Administration offers an objective to reform structures and standardize policies to promote information safeguarding. Citing "recent information breaches" (i.e., Edward Snowden, WikiLeaks) as contrary to proper information sharing *and* safeguarding, the Administration states the latter "depends on implementing and strengthening policies and procedures that enable network monitoring and detection of anomalous behavior to identify insider threats and intrusions." The Administration insists "sharing and safeguarding are not mutually exclusive" and seeks to balance the two through structures and policies that promote sharing, prevent unauthorized sharing, and protect privacy, civil rights, and civil liberties.[60] This is no small task, and begs the question whether sharing and safeguarding are in fact mutually exclusive. Perhaps a more realistic, less idealized, way of expressing the necessary relationship between sharing and safeguarding is that an acceptable balance of the two requires careful trade-offs that at times may restrict sharing in certain instances and loosen safeguarding in others, all the while ensuring a transparent, acceptable level of protection for privacy, civil rights, and civil liberties.

For courses of action and allocation of resources, the *National Strategy for Information Sharing and Safeguarding* requests an "integrated implementation plan" and lists 16 "priority objectives" for the plan to address.[61] In 2013, the National Security Staff published the *Strategic Implementation Plan*, which aligns the Strategy's 16 priority objectives with its five goals. The plan assigns actions items to "stewards" in relevant organizations within a "framework" that "provides the ability to respond to changing priorities and individual department and agency resource allocations."[62]

The information sharing strategy and implementation plan share several basic underlying assumptions and espoused cultural beliefs and values. For example, in the

---

[60] *National Strategy for Information Sharing and Safeguarding*, 7, 12-13.
[61] *National Strategy for Information Sharing and Safeguarding*, 14-15.
[62] *Strategic Implementation Plan for the National Strategy for Information Sharing and Safeguarding* (Washington: National Security Staff, December 2013), 4, 6.

first paragraph of his cover letter to the Strategy, President Obama states meeting his responsibility to secure the nation "requires the closest possible cooperation" at all levels of government and among all relevant functions.[63] The Administration values inter-agency and inter-disciplinary cooperation as a way to enhance information sharing and thereby enhance national security. In fact, "sharing" is a value evinced most forcefully by the fact an entire strategy is dedicated to it. Moreover, the Strategy builds upon recent efforts that "streamlined policies and processes, [overcame] cultural barriers, and better integrated information systems to enable information sharing," reinforcing the current value placed on information sharing.[64] The implementation plan expresses basic underlying assumptions that information sharing efforts must accord with fundamental American values and "be consistent with the Constitution and in compliance with U.S. laws and regulations."[65] These basic underlying assumptions appear consistently across each of the strategy documents reviewed in this study.

For organizational culture change, the White House promotes several mindset adjustments to improve information sharing to better secure the nation. As discussed above, the Obama Administration views information as a national asset that must be shared and safeguarded in order to be useful for national security. To share and safeguard information effectively and properly, originators and consumers must embrace responsibility and accountability in making secure information as accessible as possible for those authorized to receive and use it. Additionally, the Administration advocates for risk management instead of risk aversion in making decisions to share and safeguard information. To improve collaboration across the US government, the Administration offers an "enterprise-wide approach" that "moves stakeholders away from agency-specific networks and applications and provides secure and authorized access to information in ways that allow information sharing across departments and agencies."[66] Each of these ideas—information as a national asset, responsibility and accountability, risk management, collaboration—represent Schein-style organizational cultural values the White House seeks to instill in information sharing. In the implementation plan, the

[63] *National Strategy for Information Sharing and Safeguarding*, cover letter by President Obama.
[64] *National Strategy for Information Sharing and Safeguarding*, 1.
[65] *Strategic Implementation Plan for Information Sharing and Safeguarding*, 6.
[66] *National Strategy for Information Sharing and Safeguarding*, 7.

National Security Staff promotes adoption of a common language and transparency across all levels of government in order to increase the efficiency of requests for information. This is a practical effort that reflects a cultural change away from "stove-piped," agency-specific information rules toward the Strategy's enterprise-wide approach.

DOD Information Sharing Strategy. In 2007, the Bush Administration published the *National Strategy for Information Sharing*; a supporting *DOD Information Sharing Strategy* came into effect the same year. The DOD Chief Information Officer states the department's vision is "to deliver the power of information to ensure mission success through an agile enterprise with freedom of maneuverability across the information environment."[67] The DOD strategy provides four goals in accordance with its vision:

1. Promote, encourage, and incentivize sharing;
2. Achieve an extended enterprise;
3. Strengthen agility in order to accommodate unanticipated partners and events; and
4. Ensure trust across organizations.[68]

Of note from these fairly straightforward goals is the term "extended enterprise," which refers to the expansion and refinement of capabilities to share information internally within DOD, as well as information sharing with external departments and agencies. As an example for the latter, the DOD strategy cites the Hurricane Katrina recovery experience in 2005 where an extended enterprise for information sharing went beyond DOD to include the Department of Homeland Security, Federal Emergency Management Agency, the US Coast Guard, state and local agencies, and other entities.[69]

The Chief Information Officer advocates several approaches to achieve the Strategy's goals. Of significance here is the value DOD places on inter-departmental and inter-agency relationship-building to create "a trusted community of information sharing that promotes collaboration, leverages the information integrators in the community and reduces the 'seams' between organizations, domains and functions." For culture change across organizations, DOD acknowledges its limited ability to create such an

[67] *DOD Information Sharing Strategy*, ii, 3.
[68] *DOD Information Sharing Strategy*, iii, 5.
[69] *DOD Information Sharing Strategy*, 5.

environment; other departments and agencies must also step forward in a collaborative manner. Specifically, DOD acknowledges a basic underlying assumption "that external partners' sharing capabilities and philosophies will not necessarily conform to the DOD environment and culture."[70] Nevertheless, DOD operates in good faith and believes differences of opinion regarding a suitable information sharing environment can be bridged across a diversity of external entities.

In addition to the five approaches, the Chief Information Officer insists improvements in five "touchstones of information sharing" will assist realization of the Strategy's four goals. The Strategy identifies "Culture, Policy, Governance, Economics and Resources, and Technology and Infrastructure" touchstones and promises an implementation plan to align the approaches and touchstones effectively to achieve strategy goals. The Strategy advocates "a major cultural shift across the DOD" to achieve information sharing improvements, specifically a change from "a mindset of information '*ownership*'" to "information '*stewardship*'" (emphasis added).[71] This accords with intentional use of the term "steward" within the *Strategic Implementation Plan for the National Strategy for Information Sharing and Safeguarding* discussed above. Moreover, policies, governance structures, budgets and incentives, and supporting technologies and infrastructure must each be scrutinized and re-tooled to facilitate creation of an effective federated information sharing environment.

To assist realization of this environment through designation of courses of action and allocation of resources, the Chief Information Officer published the 2009 *DOD Information Sharing Implementation Plan*. The Implementation Plan features ten focus areas with assigned tasks to specific organizations to complete within three years in order to achieve the goals of the *DOD Information Sharing Strategy*.[72] Of note, Focus Area 2, "Instilling an Information Sharing Culture," includes tasks to "develop incentives to promote information sharing practices and procedures," reform "policies and processes that create impediments or disincentives to sharing information," and inculcate

---

[70] *DOD Information Sharing Strategy*, 2, 8.
[71] *DOD Information Sharing Strategy*, iii, 10-14.
[72] *Department of Defense Information Sharing Implementation Plan* (Washington: Office of the Assistant Secretary of Defense for Networks and Information Integration/DOD Chief Information Officer, April 2009), ii, 2-3.

information sharing cultural values in DOD education and training. Additionally, Focus Area 10 of the Implementation Plan, "Supporting DOD's Mission Needs Across Federal Information Sharing Initiatives," contains two tasks of interest: one that seeks to support and improve "information sharing across the Federal Government and with external mission partners," and another to "develop a phased strategic level Homeland Defense/Civil Support Information Sharing Plan" to facilitate sharing "among key operation centers." Overall, the Chief Information Officer acknowledges that a "cultural shift alone is not sufficient"; in addition to improving information sharing across the federal government, DOD must enhance "management, operations, classification and marking processes, identity and access management, [and] technical infrastructure" to achieve the goals of the Strategy and, more importantly, improve decision-making for actions to defend the US against an array of threats.[73]

DOD Information Enterprise Strategic Plan, 2010-2012. In 2010, the DOD Chief Information Officer published the *DOD Information Enterprise Strategic Plan, 2010-2012*, which seeks "to achieve an information advantage for our people and mission partners (including multinational partners) by leveraging net-centric information sharing."[74] The Plan identifies information as "one of our nation's greatest sources of power" and "a strategic asset" (predating the White House's similar, yet slightly different, designation of information as a national asset by two years), which prompts the creation of a useful and interactive DOD Information Enterprise to leverage the power of information throughout all mission areas.[75] The Chief Information Officer envisions a net-centric DOD Information Enterprise built from and around information, with "a set of standards, services and procedures that enable information to be widely available to authorized users" to support the full range of mission accomplishment.[76] The Plan's vision, goals, and objectives represent a determined effort to meet the intent of the

[73] *DOD Information Sharing Implementation Plan*, ii-iii, 7-8, 26-27.
[74] *Department of Defense Information Enterprise Strategic Plan, 2010-2012* (Washington: Office of the Assistant Secretary of Defense for Networks and Information Integration/DOD Chief Information Officer, May 2010), i. "Net-centric" means "relating to or representing the attributes of a robust, globally interconnected network environment (including infrastructure, systems, processes, and people) in which data are shared timely and seamlessly among users, applications, and platforms. See DODD 8000.01, 11.
[75] *DOD Information Enterprise Strategic Plan*, i.
[76] *DOD Information Enterprise Strategic Plan*, ii.

National Strategy for Information Sharing and Safeguarding.

The *DOD Information Enterprise Strategic Plan* identifies goals and objectives with key performance indicators and specific strategy elements that "guide the transformation of DoD from a stove-piped information approach to achieving the Department's net-centric information sharing vision." One relevant goal is to create "a service-oriented information enterprise where all data assets, services and information sharing solutions must be visible, accessible, understandable and trusted by all authorized users, except where limited by law, policy or security classifications." Clearly, this is a complex goal, with multiple variables that may or may not be amenable to satisfactory trade-off or balancing. DOD recognizes a duty and necessity to "share information in a timely and protected manner" with "interagency mission partners" to support "national security missions," including counterterrorism and homeland defense. This is an important commitment to partner agencies, many of which also have an interest in combating transnational organized crime. A specific objective seeks enhanced "interoperability, collaboration, and improved information sharing capabilities … between DoD and mission partners," with specific supporting strategy elements to do so, including elimination of "regulatory and cultural barriers that impede information sharing and interoperability" and "incentives to DoD activities to share information, as appropriate, with agencies, mission partners, industry, and citizens."[77] Through binding support agreements and incentivized cultural change, the DOD seeks increased and more effective information flows among relevant players in the national security arena.

A related goal of the Plan is to acquire "interoperable infrastructure" that facilitates information sharing within the DOD and with mission partners. This requires transformation of legacy "system-specific infrastructures to a shared infrastructure" that supports new "service-oriented approaches, such as cloud computing and virtualization."[78] Efficient, lower cost "cloud computing centers" will "enable data and service transparency" with "cross domain solutions (services) that enable information flow from one domain to another."[79] Upgraded infrastructure designed for information

[77] *DOD Information Enterprise Strategic Plan,* ii, 1-2, 4.
[78] *DOD Information Enterprise Strategic Plan,* 7.
[79] *DOD Information Enterprise Strategic Plan,* 1.

sharing is a worthwhile goal; yet, it is only worth the expense if other US entities also prioritize and budget to procure interoperable infrastructure that enhances two-way flows of security information. The DOD intention to lead on information sharing is clear and commendable, but the risk is that its investments will not be matched by other departments and agencies vital to a whole-of-government approach against national security threats, including transnational organized crime.

For more specific courses of action and allocation of resources, the *DOD Information Enterprise Strategic Plan* references a supplementary roadmap that aligns the plan's goals and objectives with particular activities assigned to various functional areas. The roadmap also serves a baseline function to assess DOD efforts toward meeting the goals and objectives of the Plan.[80] As a guide and measurement tool, the roadmap pushes plan implementation and overarching cultural change.

The Plan embraces organizational culture change emphatically; in fact, references to culture change permeate the Plan. The Chief Information Officer defines "culture change" as "taking new perspectives that lead to changed behavior on sharing information;" specifically, the strategic plan states that "the principles of need-to-share, breaking down silos, and developing reusable, accessible services must become hallmarks of how we [the DOD] approach information."[81] Additionally, DOD must share information generously with partners but protect it in a vigilant manner—at the same time. As noted in the national information sharing plan, this is a complicated dual task. Yet the expectation is to do so without any trade-offs.

The *DOD Information Enterprise Strategic Plan* offers several success stories for information sharing efforts. As an example of a positive development representative of culture change, the Chief Information Officer praises the "wiki approach" and use of "Intellipedia"—"the Intelligence Community (IC)-hosted social networking wiki toolset"—in the creation of the plan.[82] Additionally, the Plan cites the 2009 launch of "Universal Core (UCore)," an information exchange system developed by DOD, Department of Homeland Security, Department of Justice, and the Director of National

[80] *DOD Information Enterprise Strategic Plan*, ii.
[81] *DOD Information Enterprise Strategic Plan*, iii.
[82] *DOD Information Enterprise Strategic Plan*, i.

Intelligence, as a successful example of collaborative efforts to replace stove-piped data systems with a cost and time-saving system designed specifically to share information among partner entities.[83] These success stories promote culture change and reinforce the basic underlying assumption of the Plan: secure information sharing is a vitally important way to improve decision-making for actions to protect the nation from threats.

Strategy and Culture: Information Sharing on Transnational Organized Crime

This chapter examined key US strategy documents on transnational organized crime and information sharing using two elements of a composite theoretical framework: Chandler's *strategy* and Schein's *organizational culture*. This chapter identified basic long-term goals and objectives for each strategy document, as well as their planned courses of action and allocation of resources. This study also extracted espoused beliefs and values and basic underlying assumptions contained in the strategy documents and noted any efforts to promote organizational culture change.

Upon completion of strategy analysis, key US strategy documents represent a cumulative good-faith attempt to provide direction, guidance, and prioritization of effort for DOD toward a shared goal to improve information sharing on transnational organized crime. In general, selected strategy documents exhibit consistency for the imperative to share information effectively throughout all levels of government in the US and among various functions—law enforcement, intelligence, military, homeland security, etc.—to confront national security threats successfully, including transnational organized crime. The strategy documents recognize the need to develop effective information sharing institutions and processes through organizational agreement, infrastructure improvement, and technological compatibility. Moreover, the strategy documents express a collective belief in the synergistic power of cooperation and the need to continue to refine organizational cultures to enable optimal levels of collaboration in order to achieve maximum effectiveness against dangerous security challenges.

Of course, this chapter also exposed problems and inconsistencies within selected strategy documents that may cause difficulties in policy implementation and execution. One critical challenge in promoting change of any sort is how to incentivize others to buy into and view change as positive, possible, and worthy of supporting efforts.

---

[83] *DOD Information Enterprise Strategic Plan*, 5.

Bureaucracies are notoriously resistant to change, especially if an organization views potential change as weakening its hold on a mission or information that serves as a basis for influence, budget allocations, prestige, etc. Marcelo Bucheli, Joseph Mahoney, and Paul Vaaler point out in their praise of Chandler's monumental work on business history, *The Visible Hand*, that "innovative firms re-draw organizational boundaries and structures for efficient and effective innovation."[84] To do so, leaders must understand the forces of competition and authority at play in generating innovation. Owen Coté argues competition fuels innovation while insistence on cooperation and deference to authority limits the potential for idea generation.[85] Stephen Rosen posits that competition drives innovation within dynamic, distinct organizational cultural boundaries.[86] Barry Posen insists leaders can and should exercise their authority at times to propel the innovation process in a preferred direction.[87] Overall, market-incentivized competition stimulates novel ideas but competition without authoritative direction or regulation may lack a nexus to broader goals. Leaders must strike a proper balance between encouraging competitive environments for innovative thinking and intervening to provide timely, value-added guidance to push new ideas forward.

The problem of incentivizing innovation is no different for information sharing on transnational organized crime. Bhavani Thuraisingham identifies the lack of discussion of incentives as a key problem in his analysis of federal information sharing strategies.[88] Additionally, Michael Chau, et al., note, "Agencies are not motivated to share

---

[84] Marcelo Bucheli, Joseph T. Mahoney, and Paul M. Vaaler, "Chandler's Living History: The Visible Hand of Vertical Integration in 19th Century America Viewed Under a 21st Century Transaction Costs Economics Lens" (Champaign: University of Illinois at Urbana-Champaign, 2007), 2, http://www.business.uiuc.edu/Working_Papers/papers/07−0111.pdf.
[85] Owen R. Coté, Jr., "The Politics of Innovative Military Doctrine: The U.S. Navy and Fleet Ballistic Missiles" (PhD diss., Harvard University, February 1996), 337-338, 391.
[86] Stephen P. Rosen, *Winning the Next War: Innovation and the Modern Military* (Ithaca, NY: Cornell University Press, 1991), 19-21.
[87] Barry R. Posen, *The Sources of Military Doctrine: France, Britain, and Germany Between the World Wars* (Ithaca, NY: Cornell University Press, 1984), 224.
[88] Bhavani Thuraisingham, "Information Sharing Strategies of the United States Federal Government and Its Allies And Our Contributions Towards Implementing These Strategies" (Selected Papers in Security Studies: Volume 2, Technical Report UTDCS-23-10, Department of Computer Science, The University of Texas at Dallas, Dallas, 2 August 2010), 19.

information and knowledge if there is no immediate gain."[89] Rick Hayes-Roth, et al., also cite lack of incentives as a stumbling block for greater information sharing advances, finding a lack of empowerment for "change agents" and an absence of "overriding pressure to bring about incremental adaptive improvements" in information sharing.[90] For the strategy documents analyzed in this study, there is certainly more room for consideration of how to incentivize organizations to embrace information sharing as not only an intrinsically good idea, but a practical way to enhance counter-threat activities. Still, Hayes-Roth et al. caution against unrealistic expectations, noting the private sector has pursued information sharing improvements for over twenty years. Like the private sector, "there is significant inertia perpetuating low levels of interoperability and information sharing" in the public sector in the US and abroad.[91] US leaders must continue to "beat the drum" for information sharing until it is a more general operational reality—and then beat the drum indefinitely for constant refinement.

For transnational organized crime in general, Bjelopera and Finklea identify concerns with the lack of incentives for agencies to devote sufficient resources against the threat. Unlike specific attention-grabbing acts of terrorism (e.g., bombings, hijackings), transnational criminal organizations avoid publicity and prefer low-profile continuous criminal operations. Lacking the "negative visceral reactions" of terrorist acts, the effects of transnational organized crime are nonetheless "far-reaching," and include "impacts [to] economic stability, public health and safety, and national security."[92] The policy problem is how to incentivize various organizations from high publicity (terrorist act), high reward (thwart terrorist act) endeavors toward low publicity (transnational organized criminal activity), low reward (stop individual criminal activities). As noted in Chapter Two, the incentive may lie in convincing agencies of the high reward in dismantling large, complex, powerful, negative-influencing organizations.

---

[89] Michael Chau et al., "Building an Infrastructure for Law Enforcement Information Sharing and Collaboration: Design Issues and Challenges" (Tucson: University of Arizona Campus Repository, 2001), 3.
[90] Rick Hayes-Roth et al., "How to Implement National Information Sharing Strategy: Detailed Elements of the Evolutionary Management Approach Required" (Monterey: Calhoun Institutional Archive of the Naval Postgraduate School, 2008), 1.
[91] Hayes-Roth et al., "How to Implement National Information Sharing Strategy," 2.
[92] Bjelopera and Finklea, *Organized Crime*, 37.

To share information implies a certain level of trust between sender and recipient. A key challenge in this relationship is how to enforce discipline in those instances when information is not shared when it should be or is provided improperly in a less than secure manner. To build a culture of trust that promotes information sharing requires construction of rules and punishments applicable to individuals in multiple peer organizations. More specifically, Bruce Perry argues trust is a function of "information technology controls," where a lack of enforceable rules and punishments for information technology infrastructure "leads to an unwillingness to share information."[93] The *National Strategy for Information Sharing and Safeguarding* best recognizes the tension between trust and fear of breaches of trust in sharing information. Other key strategy documents recognize this tension also, but in total, do not provide significant detailed guidance on how to overcome this problem beyond simply working it on a case-by-case basis between organizations. As with incentives, trust is a critical component in realizing an information sharing culture based on the "need to share," not just the "need to know."[94] Individuals charged with securing sensitive information that, if compromised, could cost lives must not only be incentivized to share, they must know that sharing information carries minimal risk and information security violations will not be tolerated. Chau et al. state, "In the law enforcement domain, security is of great concern. Most of the data we deal with are highly sensitive. Improper use of data could lead to fatal consequences."[95] This is no less so for efforts against transnational organized crime. Transnational organized crime is a dangerous business for dangerous characters. More thought should be directed to specific mechanisms, agreements, and technology controls in strategy (Chandler) to instill trust in sharing processes and involved individuals in the organizational culture (Schein).

Another significant challenge involves excessive focus on specific technological solutions. Thuraisingham observes, "Technology is important, but any solution must not

[93] Bruce H. Perry, "Information Sharing Among Intelligence, Law Enforcement, and Other Federal, State, and Local Agencies" (Master's thesis, Air University, Air War College, 15 February 2008), 17.
[94] Green, "It's Mine!" 19-20; *The 9/11 Commission Report*, 417.
[95] Chau et al., "Building an Infrastructure," 3.

depend on a particular technology."[96] Emphasis on specific technologies as linchpins for strategy success—beyond citing technologies as good examples of the direction in which the strategy is moving—presents a risk the technologies may be rapidly superseded by improved technologies, which tends to diminish the credibility and forcefulness of the strategy's advocacy. This is apparent even when a strategy document is only a couple of years old. For example, the *DOD Information Enterprise Strategic Plan* lauds Intellipedia as a pivotal tool for not only creation of the strategic plan, but more importantly for information sharing among agencies in the Intelligence Community as of 2010. In fairness, the DOD Chief Information Officer cites Intellipedia as demonstrative of a valuable overall wiki approach to information sharing. Nevertheless, the risk remains that readers focus on the specific technology—which may become obsolete—over the capability the technology represents in general—which is more likely to endure.

The most troubling issue found in this analysis is DOD's uncertainty about how to treat transnational organized crime. DOD is a leading department in the promotion of information sharing, though other departments and agencies are certainly active advocates in this area as well.[97] Yet DOD strategy documents accord transnational organized crime varying levels of mention which reflects its uncertain value to the department. DOD must define mission parameters in which it accepts a general supporting role in the fight against transnational organized crime but has sufficient latitude in authorities to bring its unrivaled capabilities to bear more fully in specific instances against a threat deemed significant by national leaders.

The next chapter pivots analysis to relevant institutions and processes for information sharing involved in the fight against transnational organized crime. Using Chandler's *structure* and Schein's *organizational culture*, the intent is to scrutinize practical information sharing efforts and identify any problems that may inhibit actions—including those by DOD—to counter transnational organized crime.

[96] Thuraisingham, "Information Sharing Strategies," 20.
[97] Thuraisingham, "Information Sharing Strategies," 20.

Chapter 4

Analysis of Structures for Information Sharing on Transnational Organized Crime

This chapter analyzes specific structures involved in US efforts against transnational organized crime. Structures should serve to translate US strategy documents into reality through functional organizations with appropriate resources to conduct activities in accordance with strategic direction. This analysis seeks to determine if structure follows strategy in promoting effective information sharing on transnational organized crime by the US government in general and DOD in particular. The structure and culture elements of this study's composite theoretical framework guide analysis of select structures relevant to transnational organized crime. First, Chandler's notion of *structure* assists in determining whether institutions involved in sharing information on transnational organized crime have clear "lines of authority and communication" that enable an effective "flow" of "information and data." Next, Schein's *organizational culture* model helps identify espoused beliefs and values or basic underlying assumptions that relevant structures represent and promote. As with strategy, Schein's model provides a lens to view organizational cultural change within the structures under analysis. This chapter analyzes organizations pivotal to DOD involvement in information sharing efforts against transnational organized crime: Special Operations Division, El Paso Intelligence Center, and Joint Interagency Task Force South. The discussion then offers an overall assessment of the current cumulative structure in place to support the enterprise against transnational organized crime and information sharing efforts within it.

Structure and Culture: SOD, EPIC, and JIATFS

Special Operations Division. The *Strategy to Combat Transnational Organized Crime* identifies several US entities as particularly important for information sharing efforts in the fight against transnational organized crime. The first entity mentioned is the secretive Virginia-based Special Operations Division (SOD), a "multi-agency operations coordination center" led by the Drug Enforcement Administration (DEA) since 1994.[1] SOD includes representatives from over 20 agencies, including local, state,

[1] *Strategy to Combat Transnational Organized Crime,* 18.

federal, and international law enforcement agencies, the Intelligence Community, and DOD. SOD pursues drug trafficking and narco-terrorism organizations and focuses "sophisticated technology and investigative intelligence resources of its participating law enforcement and intelligence agencies" specifically on "efforts to disrupt and dismantle the command and control elements" of targeted organizations.[2] SOD shares information obtained through collective efforts with foreign and domestic partners who then pursue targeted individuals and organizations to the full extent of their authorities and capabilities.[3] For example, in 2012 the DEA announced the results of "Project Below the Beltway," a two-year SOD-driven initiative that "combined 411 investigations in 79 United States cities and 12 foreign cities to target the Sinaloa and Juarez Cartels and other drug-trafficking organizations and gangs throughout Mexico and the United States."[4] In addition to support for foreign law enforcement activities on multiple continents, SOD coordinated the investigative efforts of numerous federal, state, and local law enforcement agencies in the US, including the FBI, Internal Revenue Service, Immigrations and Customs Enforcement (ICE), Customs and Border Protection, US Marshals Service, and Office of Foreign Asset Control.[5] Impressive investigative results included "3,780 arrests and the seizure of 6,100 kilograms of cocaine, 10,284 pounds of methamphetamine, 1,619 pounds of heroin, 349,304 pounds of marijuana, and nearly $150 million in United States currency."[6]

SOD represents an example of the "lead agency" construct for interagency activities. The DEA is ultimately responsible for the success or failure of SOD in its mission. Aside from DEA employees, SOD lacks command authority to enforce

---

[2] Statement of Derek S. Maltz, Special Agent in Charge, Special Operations Divisions, Drug Enforcement Administration, before the Subcommittee on Terrorism, Nonproliferation, and Trade, Committee on Foreign Affairs, US House of Representatives, "Narcoterrorism and the Long Reach of U.S. Law Enforcement, Part II," 17 November 2011, 1, 3, 4, 7; *Strategy to Combat Transnational Organized Crime*, 18.

[3] *Strategy to Combat Transnational Organized Crime*, 18.

[4] Statement of the Honorable Michele Leonhart, Administrator, Drug Enforcement Administration, before the Subcommittee on Commerce, Justice, Science and Related Agencies, Committee on Appropriations, US House of Representatives, 2 April 2014, 11.

[5] Drug Enforcement Administration Public Affairs, "'Project Below the Beltway' Targets Sinaloa and Juarez Cartels and Affiliated Violent Street Gangs Nationwide," 6 December 2012, http://www.dea.gov/divisions/hq/2012/hq120612.shtml (accessed 23 February 2015).

[6] Leonhart, 2 April 2014, 11.

cooperation and information sharing among participating agencies. Individual agencies can adjust their level of participation up or down based on other mission priorities, budgetary resources, etc., which poses a risk to SOD's effectiveness that might not exist in a more integrated, directive interagency construct. As an example of the fragility of SOD's ability to ensure cooperation, a 2009 Government Accountability Office (GAO) report identified problems between ICE and SOD. Specifically, the report noted that ICE provided limited information to SOD based on "an outdated interagency agreement" specifically and "long-standing disputes involving ICE's drug enforcement role and DEA's oversight of that role" generally.[7] Without information from ICE, SOD lacked visibility on a substantial number of ICE investigations and operations related possibly to SOD efforts, posing significant de-confliction issues (including agent and source safety) and the potential for missed investigative opportunities. It appears ICE improved its information sharing with SOD since 2009, exemplified by DEA's acknowledgement of ICE participation in Project Below the Beltway. Nevertheless, interagency competition and lack of unity of command challenge SOD efforts to promote full cooperation and information sharing for the collective benefit of all participating agencies in efforts against drug trafficking and narco-terrorism.

While SOD lacks unity of command, it achieves unity of effort based on expected benefits of continuing cooperation and information sharing by participating agencies. If agencies wish to maintain access to the collective resources and intelligence of SOD to drive successful investigations and operations, an expectation to reciprocate information sharing must be met. In terms of Chandler's structure, SOD's lines of authority appear complex and weak as a coordination center, yet strong incentives promote open lines of communication that enable effective flows of information and data among agencies.

The danger in a lead agency construct lies where the lead agency takes all the credit for success, de-incentivizing cooperation by participating agencies. In this case, the DEA appears to be avoiding this pitfall with SOD, voicing its appreciation for participating agencies and lauding their contributions to Congressional audiences. For

[7] Government Accountability Office, *Report to the Co-Chairman, Caucus on International Narcotics Control, U.S. Senate: Drug Control, Better Coordination with the Department of Homeland Security and an Updated Accountability Framework Can Further Enhance DEA's Efforts to Meet Post-9/11 Responsibilities*, GAO-09-63 (Washington: GAO, March 2009), i.

example, Special Agent Derek Maltz, SOD Special Agent in Charge, stated to a Congressional sub-committee in 2011, "We are extremely proud of our close, cooperative relationships with State and Local law enforcement, as well as our Federal counterparts." Maltz highlighted the "close coordination and open sharing of counternarcotics and counterterrorism intelligence, among law enforcement agencies and the Intelligence Community," adding "this synergistic relationship is one of the reasons SOD was established" to realize "benefits of interagency cooperation and intelligence sharing."[8]

In addition to representing DEA's willingness to share credit for SOD successes, such statements also reflect beliefs, values, and underlying assumptions. DEA leadership believes in cooperation and information sharing in a collaborative entity like SOD based on proven value. SOD leaders express appreciation for participating agencies publicly in order to motivate further cooperation, based on the assumption that past success will generate future success. Department of Justice (DOJ) and DEA leadership appear to believe in the power of interagency action. The Office of the Attorney General identifies SOD as "another lynchpin in the Department's effort to coordinate tactical intelligence and operation[al] information across components and agencies."[9] More generally, DEA Administrator Michele Leonhart stated to a Congressional sub-committee in 2014, "Intelligence sharing, de-confliction, and cooperation between Federal, state, and local law enforcement partners is the key to combating transnational organized crime."[10] The DEA Administrator cited SOD as a successful example of information sharing and also lauded the efforts of another DEA entity, the El Paso Intelligence Center (EPIC).

***El Paso Intelligence Center*.** DEA manages EPIC, an entity established in 1974 in El Paso, Texas, to support trafficking and smuggling interdiction efforts. Since that time, and especially after 9/11, EPIC expanded into "an all threats center with a focus on the Western Hemisphere, and a particular emphasis on the Southwest border, that leverages the authorities and expertise of its partners to deliver informed intelligence."[11]

---

[8] Maltz, 17 November 2011, 3-4.
[9] Department of Justice, *FY 2010 Performance and Accountability Report* (Washington: Office of the Attorney General, November 2010), IV-36.
[10] Leonhart, 2 April 2014, 11.
[11] Drug Enforcement Administration, "Intelligence Topics at DEA: El Paso Intelligence Center," http://www.dea.gov/ops/intel.shtml#EPIC (accessed 23 February 2015).

According to a 2010 DOJ Inspector General (IG) report, "EPIC's mission has evolved in response to a shift in focus to Southwest border smuggling and associated violence, and the need for improved collaboration and timely information sharing among law enforcement and intelligence agencies."[12] EPIC supports federal, state, local, and international law enforcement partners to enhance investigations and operations against a variety of criminal activities. EPIC facilitates collaboration and information sharing through face-to-face interaction by representatives from 25 different agencies—including DOD—and 24-hour access to 74 law enforcement databases for over 19,000 authorized users. In fiscal year 2011, EPIC responded to 333,000 requests for information and supported over 18,000 investigative cases.[13]

Like SOD, EPIC represents the lead agency construct for interagency activities; DEA is ultimately responsible for the success or failure of EPIC. EPIC also lacks command authority to enforce collaboration and information sharing among represented agencies. Yet there is a key difference in mission between SOD and EPIC: SOD coordinates operations while EPIC serves a supporting role as an intelligence center. In any event, both SOD and EPIC rely on voluntary participation and reciprocal benefits among agencies to achieve unity of effort. This places EPIC in a difficult position since the 2013 *National Southwest Border Counternarcotics Strategy* identifies EPIC as the "key node" for "establishing a criminal intelligence and information sharing network."[14] In this respect, EPIC may be the closest transnational organized crime analog to the National Counterterrorism Center (NCTC; see discussion in Chapter 5). Unlike NCTC, and as noted above, EPIC lacks authorities to compel compliance by member agencies, which contributes to multiple problems for effective information sharing via EPIC.

While noting the high value attributed to EPIC by partners and product users, DOJ IG identified several issues that inhibit effective information sharing through EPIC. The following observations exemplify the types of problems interagency entities face:

---

[12] Department of Justice, *Review of the Drug Enforcement Administration's El Paso Intelligence Center* (Washington: Office of the Inspector General, June 2010), i.
[13] Larry Villalobos and Carlos Almengor, "DEA Museum Lecture Series – An Overview of the El Paso Intelligence Center," 1 December 2011, http://www.deamuseum.org/education/transcripts/EPIC-120111.pdf (accessed 26 February 2015), 10, 16; DOJ, *El Paso Intelligence Center*, i.
[14] *National Southwest Border Counternarcotics Strategy* (Washington: Office of National Drug Control Policy, 2013), 12.

- EPIC does not have an effective program or strategy to inform users and potential users about products and services that could assist them.
- The lack of an up-to-date agreement between EPIC and its participating members has contributed to coordination problems, such as member agencies not sustaining programs, sharing information, or contributing resources to EPIC.
- EPIC has not developed the National Seizure System into a comprehensive database into which all drug seizures are reported nationwide.
- EPIC has not established itself as the hub for the High Intensity Drug Trafficking Area (HIDTA) program.
- EPIC's coordination with federal and state intelligence organizations across the country is inconsistent.[15]

DOJ IG recommends several measures to improve EPIC's contributions to information sharing efforts for transnational organized crime, to include the following:

1. EPIC expand its outreach and education program to promote the use of its products and services …
2. EPIC update its Principals Accord or adopt a comparable multi-agency framework that formalizes each member's roles and responsibilities for implementing and sustaining EPIC's programs …
3. EPIC promote more complete reporting of drug seizure data to the National Seizure System …
4. The Office of the Deputy Attorney General work with the ONDCP [Office of National Drug Control Policy] to establish policy or guidance requiring HIDTAs to implement data and information sharing provisions to establish EPIC as their hub for seizure and drug movement information.
5. EPIC establish points of contact at all national, regional, state, and local fusion centers to enhance information sharing and use of EPIC's services and products.[16]

The issues identified and remedies offered by DOJ IG appear justified and supported with sufficient reported evidence. However, one issue and a related recommendation deserve further explanation. EPIC's relationship with the HIDTA program involves different parent organizations: DEA and ONDCP, respectively. Despite EPIC's stated desire to serve as the intelligence hub for the HIDTA program, EPIC cannot compel 28 regional

[15] Department of Justice, *El Paso Intelligence Center*, ii, 13, 16.
[16] Department of Justice, *El Paso Intelligence Center*, ix, 45-46.

HIDTA Intelligence and Investigative Support Centers to treat EPIC as their hub without DEA and ONDCP concurrence and influence with the HIDTA centers.[17] It remains to be seen if EPIC can serve, at a minimum, as the hub for one partner organization (HIDTA centers), let alone as the grander "key node" role for all agencies involved with counternarcotics along the Southwest border and beyond as envisioned by ONDCP.

Like SOD, EPIC's lines of authority appear complex and weak as an intelligence center, but incentives exist to establish open lines of communication that enable effective information flows among participating agencies. EPIC must continue to improve internal operations, products, and marketing to enhance its credibility as a valuable center that deserves full cooperation by relevant agencies to share information on transnational organized crime—even in the absence of authorities compelling agencies to do so.

EPIC values its identity as "an all threats center" and believes "the key to EPIC's success is a culture that transcends parochialism. EPIC is a team approach. Collectively, we deter threats and protect our nation."[18] These espoused beliefs and values reflect EPIC's organizational cultural evolution: from a limited focus on trafficking and smuggling along the Southwest border with support provided to law enforcement within the region, to an all-threats mission encompassing a wide range of crimes (including terrorism) involving border transit with support provided nationwide and internationally to partner agencies and authorized users. EPIC continues to expand its pool of partner agencies and users to increase information sharing capabilities to defeat threats. EPIC also encourages other entities to leverage its capabilities more fully, as exemplified by its desire to be the hub for HIDTA centers. Each aspect of organizational culture change pursued by EPIC must be supported with effective actions to demonstrate credibility, commitment, and reciprocal value to partners. Positive developments since publication of the DOJ IG report include creation of a Joint Collections Management Unit at EPIC "to coordinate requests for information and the dissemination of intelligence," improved information sharing capabilities with SOD and state and local law enforcement agencies, and establishment of a Border Intelligence Fusion Section (BIFS).[19]

---

[17] Department of Justice, *El Paso Intelligence Center*, 27.
[18] DEA, "Intelligence Topics at DEA," http://www.dea.gov/ops/intel.shtml#EPIC.
[19] *National Southwest Border Counternarcotics Strategy*, 11.

In addition to SOD and EPIC, the *Strategy to Combat Transnational Organized Crime* makes specific mention of the EPIC BIFS. While EPIC is a DEA-led entity, the Department of Homeland Security (DHS) is the lead agency for BIFS. Established in 2010, the mission of BIFS is to support US law enforcement investigations and operations along the Southwest border through provision of "all-source, all-threats criminal intelligence."[20] At first glance, BIFS appears redundant to the overall mission of EPIC. However, BIFS augments EPIC with intelligence capabilities and information from the Departments of Homeland Security, Justice, and Defense, as well as the Intelligence Community. BIFS analyzes and fuses intelligence and information gathered from EPIC's partners and various databases to generate common intelligence and operating pictures for collaborative efforts against transnational organized crime.[21] As part of the collaboration, DOD supports BIFS with analysis and training resources "to enhance intelligence and information sharing capabilities and processes associated with the Southwest border."[22] In exchange, DOD benefits from increased information sharing with the Intelligence Community and other federal agencies through a favorable relationship with BIFS, leveraging its valuable "clearinghouse of information" analyzed from various agency perspectives and fused from multiple intelligence inputs.[23]

BIFS's establishment in 2010 coincided with the release of a DOJ IG report critical of information sharing between ICE, DEA, and the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) in "Project Gunrunner," an ATF-led effort to interdict firearms trafficking between the US and Mexico. Shortly after BIFS came online, the US Congress published a report highly critical of intra- and inter-agency information sharing by ATF and DOJ in "Operation Fast and Furious," a part of Project Gunrunner that received significant public criticism in the aftermath of the murder of a US Border Patrol

---

[20] *National Southwest Border Counternarcotics Strategy*, 11.
[21] *Strategy to Combat Transnational Organized Crime*, 19; *National Southwest Border Counternarcotics Strategy*, 11.
[22] Statement of the Honorable Paul Stockton, Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs, before the Subcommittee on Border and Maritime Security, Committee on Homeland Security, US House of Representatives, 17 April 2012, 7.
[23] Adam Isacson, George Withers, and Joe Bateman, "An Uneasy Coexistence: security and migration along the El Paso-Ciudad Juarez border," Washington Office on Latin America, 20 December 2011, http://www.wola.org/commentary/an_uneasy_coexistence (accessed 24 February 2015), 10.

agent in 2010 with a weapon "trafficked" by ATF in efforts to expose firearms trafficking networks and movements.[24] The creation of BIFS may represent part of an effort to close perceived gaps in information sharing among agencies and entities—including SOD and EPIC—involved in Project Gunrunner and other efforts against transnational criminal organizations. While BIFS strives to enhance the level of intelligence fusion and information sharing for operations along the Southwest border, Joint Interagency Task Force South (JIATFS) represents a decades-old interagency model for effective intelligence fusion, timely information sharing, and successful interdiction operations against drug traffickers in and around Central and South America.

Joint Interagency Task Force South. Based in Key West, Florida, JIATFS is a drug interdiction organization composed of members from 18 US military, law enforcement, and intelligence agencies, as well as liaison officers from 14 partner nations. The JIATFS mission is to "conduct interagency and international Detection & Monitoring operations, and facilitate the interdiction of illicit trafficking and other narco-terrorist threats in support of national and partner nation security." JIATFS's vision is to "be the center of excellence for all-resource fusion and employment of joint, interagency, and international capabilities to eliminate illicit trafficking posing a threat to national security and regional stability."[25] JIATFS's enormous area of responsibility totals 42 million square miles and includes the Caribbean basin, Central America, South America, South Atlantic Ocean, and southeastern Pacific Ocean. JIATFS's operating area mirrors that of its parent organization, US Southern Command, but also includes oceanic portions of US Northern Command, US Pacific Command, and US European Command.[26] This overlapping operating area challenges JIATFS and US Southern Command leaders in interactions with each other and external geographic combatant commands to coordinate and de-conflict operations with minimal friction.

---

[24] Matthew F. McDonald, "Joint Interagency Task Force-Illicit Trafficking: Enhancing the Interagency Organizational Framework for Operations along the Southwest Border" (Master's thesis, US Marine Corps Command and Staff College, 1 May 2012), 2-4.
[25] Joint Interagency Task Force South, "Joint Interagency Task Force South: Serving the Nation for Over 20 Years," http://www.jiatfs.southcom.mil/index.aspx (accessed 24 February 2015).
[26] Evan Munsing and Christopher J. Lamb, *Joint Interagency Task Force-South: The Best Known, Least Understood Interagency Success* (Washington: National Defense University Press, June 2011), 23, 29; Joseph Perry and Cory Riesterer, "Joint Interagency Task Force South: Combating illicit drug operations," *Proceedings* 71, no. 3 (Fall 2014): 48.

While subordinate to US Southern Command, JIATFS is also considered a national task force. According to a JIATFS official, "the 'national' concept provided for an organizational structure, which recognized the force multiplier effect that could be realized from a task force manned and led by personnel from various agencies with a drug interdiction mission."[27] This designation allows JIATFS to exercise tactical control over personnel and resources from any partner agency. Though less than the operational and administrative control held typically by military commanders, the level of control exercised by JIATFS is nevertheless considerable compared to the lead agency constructs of SOD and EPIC. To paraphrase John Fishel, JIATFS has "structural," not authoritative, unity of command based on the voluntary nature of the interagency construct.[28] Tom Stuhlreyer views JIATFS as a "coalition of the willing," with partner agency deference to the task force's unity of command only up to the point it conflicts with partner agency interests.[29] For JIATFS, the trade-off in foregoing full military-style unity of command or lead agency status is greater access to invaluable interagency resources, which enables more effective efforts to interdict traffickers.

Though complex, JIATFS's various lines of authority serve as a source of strength. JIATFS is the only entity authorized to conduct interdiction operations within its area of responsibility. JIATFS leverages lack of jurisdictional competition and ownership of a target-rich environment to incentivize cooperation by numerous agencies eager to take advantage of opportunities found only within JIATFS. The task force then applies the collective power of multiple agencies' legal authorities, specialized assets and information, and diverse personnel expertise to a dynamic operating environment.[30]

JIATFS's integrated organizational structure and intelligence fusion process promote open lines of communication that enable effective flows of information and data

---

[27] Allen G. McKee, quoted in Robert A. Remsing, "'Seams' of Inefficiency and Joint Interagency Task Force (JIATF) Operations" (Master's thesis, Naval War College, 16 May 2003), 5.
[28] John T. Fishel, "The Interagency Arena at the Operational Level: The Cases Now Known as Stability Operations," in *Affairs of State: The Interagency and National Security*, ed. Gabriel Marcella (Carlisle: Strategic Studies Institute, December 2008), 429; Robert S. Pope, "Interagency Task Forces: The Right Tools for the Job," *Strategic Studies Quarterly* 5, no. 2 (Summer 2011): 120.
[29] Tom Stuhlreyer, "The JIATF Organization Model: Bringing the Interagency to Bear in Maritime Homeland Defense and Security," *Campaigning* (Spring 2007), 42.
[30] Munsing and Lamb, *Joint Interagency Task Force-South*, 39.

among partner agencies and enhance unity of effort for mission accomplishment. Partner agency personnel fill positions from top to bottom in a unique, mixed organizational hierarchy, which "promotes trust and facilitates the sharing of law enforcement investigative information … critical for any intelligence-driven organization."[31] Currently, a US Coast Guard flag officer holds the directorship for JIATFS, with a US Navy flag officer as deputy director and a Customs and Border Protection (CBP) officer as vice director.[32] JIATFS leadership reflects a merger of DHS and DOD interests, an integration that expands to include all partner agencies throughout task force positions.

Representing a dual-purpose law enforcement and military organization, Coast Guard leadership of JIATFS offers certain advantages. The Coast Guard's ability to navigate in DOD and DHS bureaucratic and operational environments provides JIATFS leadership and representatives credibility with both military servicemembers and law enforcement officials. While DOD is the statutorily-designated "lead agency for the detection and monitoring of drug trafficking into the US," the Coast Guard is the "lead agency for the interdiction and arrest of drug traffickers."[33] In practice, this means JIATFS engages DOD personnel and resources (e.g., ships, aircraft, intelligence systems) in conjunction with the Coast Guard and other agencies until actual interdiction or arrest is necessary; at that point, JIATFS uses non-DOD assets operating under law enforcement authorities to conduct interdiction activities and effect arrests and searches.

To cue interdiction resources into action requires real-time fused intelligence. JIATFS draws on extensive intelligence and information resources from partner agencies to generate effective cues. In addition to organic radar and intelligence assets, JIATFS resources include multi-source intelligence from DEA, ICE, FBI, Central Intelligence Agency, Defense Intelligence Agency, Coast Guard Intelligence Center, National Security Agency, National Reconnaissance Office, National Geospatial Intelligence Agency, EPIC, and CBP's Air and Marine Operations Center, not to mention intelligence

[31] Richard M. Yeatman, "JIATF-South: Blueprint for Success," *JFQ Forum* 42, no. 3 (2006): 26.
[32] Joint Interagency Task Force South, "Command Group," http://www.jiatfs.southcom.mil/index-1.aspx (accessed 24 February 2015); Pope, "Interagency Task Forces," 119.
[33] Munsing and Lamb, *Joint Interagency Task Force-South*, 10.

resources from US military services and partner nations.[34] Two Coast Guard officers assigned to JIATFS assert, "The physical presence of all these organizations under a single command structure allows increased face-to-face interaction and expedited information fusion to create more complete domain awareness."[35] JIATFS uses 12 distinct fusion cells to analyze and combine various information streams—with input from operations personnel—into a useful common operating picture. Evan Munsing and Christopher Lamb conclude, "The ability to control and integrate diverse intelligence sources increases the impact of any given intelligence source, including human intelligence, and allows JIATF–South to use its scarce operational assets to best effect."[36]

Statistics for interdiction efforts from 1989 to 2009 (which includes operations under previous organizational names) evince the effectiveness of JIATFS's refined intelligence-driven operations model. According to Admiral James Stavridis, former Commander of US Southern Command, JIATFS personnel seized 2,300 metric tons of cocaine and 705,000 pounds of marijuana, arrested 4,600 suspected traffickers, captured nearly 1,100 vessels, and seized approximately $190 billion from drug trafficking organizations. Adm Stavridis notes that "in 2008, JIATF-South was responsible for greater than 50 percent of the total cocaine seizures in the world."[37] The long-term impact of JIATFS interdiction efforts on the drug supply and demand is debatable; however, the impact of JIATFS on drug cartels and other transnational criminal organizations is irrefutable. While Fishel asserts, "JIATF-S is highly successful in achieving operational unity of effort regardless of its ability to affect the flow of illicit drugs into the United States," it is clear JIATFS personnel inflict significant profit losses and force otherwise unnecessary operations, logistics, and supply adaptations on the cartels.[38] Beyond the specific value in successful intelligence-driven interdiction operations, JIATFS offers an organizational model for potential emulation by entities charged with information sharing to confront national security threats.

---

[34] Munsing and Lamb, *Joint Interagency Task Force-South*, 24, 27, 70; Pope, "Interagency Task Forces," 119; GAO, *Drug Control*, 47; Yeatman, "JIATF-South," 26-27.
[35] Perry and Riesterer, "Joint Interagency Task Force South," 50.
[36] Munsing and Lamb, *Joint Interagency Task Force-South*, 70.
[37] James G. Stavridis, *Partnership for the Americas: Western Hemisphere Strategy and U.S. Southern Command* (Washington: National Defense University Press, 2010), 68.
[38] Fishel, "The Interagency Arena at the Operational Level," 437.

In JIATFS, agencies invest as partners in the interagency construct, in contrast to agency participation or representation in lead agency constructs like SOD and EPIC. The partnership starts with the integrated organizational structure but does not end there. As with SOD, JIATFS partners appreciate the value of information sharing among a large, diverse pool of organizations and the power of collective resources in unified efforts against drug traffickers. Partner agencies recognize JIATFS as "an unbeatable force multiplier" that yields "a high return on investment."[39] Since JIATFS's success is their success, they can cite contributions to JIATFS operations in departmental and Congressional budgetary processes to advocate for continued or increased resource funding. Perhaps even more than SOD, JIATFS shuns credit and prefers to attribute success to partner agencies (or declines to give credit depending on the sensitivities of the agency or partner nation).[40] This reflects an effective way to incentivize continual support from diverse agencies and avoids the appearance of DOD or DHS using other entities for parochial benefits. Additionally, JIATFS accommodates different metrics among partner agencies (e.g., amount of seizures, arrests and prosecutions), which also incentivizes support that is "key to unity of effort" and continued task force success.[41]

JIATFS values partnership and, like SOD, believes fundamentally in the power of interagency action. By definition, JIATFS cannot be an interagency entity without partner agencies and nations to fill its integrated organizational structure. One of its stated goals is to "expand to include all critical International and interagency partners."[42] Even with agency growth over the years, JIATFS continues to pursue additional partners to add capabilities and broaden the power base and influence of the task force. Partnership implies trust, respect, and cooperation.[43] JIATFS seeks to inculcate these attributes (or basic underlying assumptions) and thereby strengthen its organizational culture. Without these attributes, partnership cannot develop, thrive, and continue to evolve in a positive direction. Without partnership, JIATFS's interagency construct—

---

[39] Munsing and Lamb, *Joint Interagency Task Force-South*, 72.
[40] Munsing and Lamb, *Joint Interagency Task Force-South*, 1, 45.
[41] Yeatman, "JIATF-South," 26.
[42] JIATFS, "Joint Interagency Task Force South," http://www.jiatfs.southcom.mil/index.aspx.
[43] Reinaldo Rivera, "The Joint Interagency Task (JIATF) Conundrum: Cooperation among Competitors, is harmony achievable through trust and understanding?" (Master's thesis, Naval War College, 3 February 2003), 9, 17.

which the task force believes in, values, and assumes to be the best way to organize and operate—cannot continue to achieve buy-in and succeed in sharing information, fusing intelligence, and interdicting traffickers. In short, as Matthew McDonald concludes, "interagency partnerships serve as the key to JIATF-South's success."[44]

Partnership in JIATFS cannot be taken for granted, despite strong incentives for agencies to maintain collaboration and operational contributions. As with SOD and EPIC, agencies volunteer personnel and resources but can also pull personnel and resources to accomplish other priority missions. For example, Munsing and Lamb note that multiple agencies, including DOD and FBI, pulled resources from JIATFS after 9/11 to re-purpose them toward counterterrorism efforts. In response, JIATFS refined its intelligence cueing processes to increase targeting accuracy and seizures despite reduced partner agency resources.[45] Like SOD and EPIC, it is likely no accident that JIATFS also expanded its mission to include efforts against narco-terrorism, a development intended to entice agencies to continue partnering in a post-9/11 national security atmosphere dominated by counterterrorism efforts and associated funding.

The expanded mission of JIATFS represents an organizational culture change to keep pace with a dynamic threat environment and remain a relevant tool for national leaders. Beyond the task force itself, Munsing and Lamb assert that JIATFS constitutes a "national experiment" in organizational culture change.[46] JIATFS evolved over decades—with progression and regression along the way—until it developed an integrated structure and organizational culture that many consider a very effective, exemplary interagency model. For example, Adm Stavridis identifies JIATFS as "*the* gold standard for future joint and combined interagency and international security organizations" (emphasis in original), an assessment supported by others.[47] His successor at US Southern Command, General Douglas Fraser, considers JIATFS "the linchpin in U.S. counterdrug efforts."[48] GAO identifies US Southern Command as a

[44] McDonald, "Joint Interagency Task Force-Illicit Trafficking," 21.
[45] Munsing and Lamb, *Joint Interagency Task Force-South*, 27, 29.
[46] Munsing and Lamb, *Joint Interagency Task Force-South*, 6.
[47] Stavridis, *Partnership for the Americas*, 185; Munsing and Lamb, *Joint Interagency Task Force-South*, 1, 3, 85; McDonald, "Joint Interagency Task Force-Illicit Trafficking," 21.
[48] Posture Statement of General Douglas M. Fraser, Commander, US Southern Command, before the Armed Services Committee, US House of Representatives, 6 March 2012, 3.

success story for interagency cooperation, undoubtedly based in part on the organization and performance of JIATFS.[49] Joseph Perry and Cory Riesterer cite JIATFS as "the premier example for international and interagency partnerships in the Western Hemisphere."[50] Robert Pope also observes that multiple writers view JIATFS as the "benchmark interagency organization to emulate."[51] Over a span of 20 years, JIATFS established a highly effective organizational structure and culture that it continues to refine as necessary to adapt to dynamic threats in its area of responsibility.

Yet the motivational sense of purpose described by personnel at JIATFS reflects the organization's continuing focus on its original core mission—interdiction of cocaine traffickers.[52] While JIATF's mission statement now includes a more expansive reference to interdiction of illicit trafficking and other narco-terrorist threats, JIATFS is still geared to a narrow slice of transnational organized crime: cocaine traffickers and distributers originating in Latin America and operating primarily in the maritime and air domains. Use of JIATFS as a template for interagency information sharing on transnational organized crime across more diverse domains must account for these contextual factors.

Structure and Culture: Information Sharing on Transnational Organized Crime

This chapter examined three key US structures involved in efforts against transnational organized crime: SOD, EPIC, and JIATFS. The analysis used two elements of a composite theoretical framework—Chandler's *structure* and Schein's *organizational culture*—to (1) determine whether the three structures have clear lines of authority and communication that enable effective flows of information and data; (2) identify espoused beliefs, values, and basic underlying assumptions that relevant structures represent and promote; and (3) recognize organizational cultural change within the structures. The analysis of SOD, EPIC, and JIATFS enables an overall assessment, including critical observations, of the current cumulative structure in place to support the enterprise against transnational organized crime and information sharing efforts within it.

---

[49] Government Accountability Office, *Interagency Collaboration: Key Issues for Congressional Oversight of National Security Strategies, Organizations, Workforce, and Information Sharing*, GAO-09-904SP (Washington: GAO, September 2009), 26.
[50] Perry and Riesterer, "Joint Interagency Task Force South," 48.
[51] Pope, "Interagency Task Forces," 119.
[52] Munsing and Lamb, *Joint Interagency Task Force-South*, 36.

The structures reviewed in this chapter represent different interagency models for lines of authority and communication to enable information sharing on transnational organized crime threats: lead agency (SOD and EPIC) and integrated (JIATFS). The structures' functions also vary: an operations coordination center, intelligence center, and operational task force. A diversity of interagency models and functions involved in efforts against transnational organized crime is no weakness. On the contrary, while entities must guard against overlapping or duplicative efforts, it is advantageous for entities to develop unique capabilities, compete, and adapt based on other entities' successes and failures to enhance efforts against threats. Chandler states, "The key theme for any business is learning its boundaries: relating the firm, the markets, and the technology to your particular strengths."[53] The strength of the enterprise to combat transnational organized crime lies in recognition and promotion of the internal specialization and diversity of competitive sub-structures—interagency entities. Although lacking traditional unity of command, effective interagency entities foster a focus on unity of effort that is mutually-reinforcing and beneficial to whole entities and individual agencies. The value of the work accomplished by an interagency entity motivates and incentivizes individual agency cooperation despite the absence of a traditional, hierarchical unity of command. Conversely, in the interagency marketplace, an indicator of problems with the purpose or mission of a specific entity is low or declining individual agency investment and participation (e.g., EPIC in 2010).

This chapter's analysis revealed successes and challenges in translating strategy on transnational organized crime and information sharing into structures that conduct activities in accordance with strategic direction. The current cumulative structural arrangement meets the intent of the whole-of-government approach in the *Strategy to Combat Transnational Organized Crime*. A relatively horizontal, diffuse network of interagency entities shares information across entities to combat transnational organized crime networks, and works continually to refine information sharing and cooperation with combined resources. Since individual agencies retain their independence and unique

[53] Alfred Chandler quoted in Art Kleiner, "Chandler's Revolution," *Strategy + Business*, 9 April 2002, 3, http://digitaledition.strategy-business.com/article/Professor+Chandler%E2%80%99s+Revolution/1482870/171835/article.html# (accessed 14 April 2015).

authorities and capabilities while cooperating with interagency entities, the arrangement also remains true to the spirit and intent of separation of powers in the US Constitution. In line with American cultural values, the US government continues (correctly) to promote cooperation—not consolidation—of powers to address threats.

Regarding the espoused beliefs, values, and basic underlying assumptions relevant structures promote, this chapter focused on indicators that agencies value information sharing and interagency cooperation. It appears SOD, EPIC, and JIATFS believe genuinely in the benefits of information sharing and interagency cooperation to confront threats, which may reflect entrenchment of post-9/11 cultural shifts based on counterterrorism lessons learned (see next chapter). Examples abound of leaders citing the vital importance of cooperation and information sharing to successful investigations and operations against transnational criminal organizations. Still, interagency entities and individual agencies—including DOD—must continue to address information sharing problems and cooperation shortcomings, such as those identified in this chapter, in order to continually increase effectiveness against transnational organized crime threats.

In addition to cultural emphasis on cooperation and information sharing, interagency entities also pursue organizational changes to adapt to dynamic threats, expanding abilities to address a wider range of transnational organized crime. Flexibility in capabilities and authorities is a positive attribute for interagency entities. However, the potential pitfall here is mission creep, with entities chasing continued relevance through broadened missions against the full range of transnational organized crime threats. Based on the need to strike a healthy balance between competitive environments for innovative thinking and value-added authoritative guidance, it is more advantageous for the US government to fund a diverse array of entities working against different aspects of the complex transnational organized crime phenomenon than to have duplication of efforts by entities seeking hegemony as the only tool capable of addressing the entire range of transnational organized crime. Gaps in coverage against emerging transnational threats can be addressed as they are identified, either by innovative interagency entities that find novel ways to use their existing capabilities and authorities against new threats or through entities persuading national leadership to provide additional tools to meet new challenges.

To close this chapter with a focus on DOD, its interagency efforts appear significant and commendable. JIATFS does not succeed "without the military organizational backbone contributed by DOD."[54] Interagency efforts along the Southwest border rely on support from DOD. DOD participates in SOD, EPIC, and BIFS. In short, DOD embraces whole-of-government and whole-of-nation approaches in accordance with national and DOD strategy guidance. Of course, it can be argued DOD funding allows great leeway to support and participate in more interagency entities compared to other less-funded departments and agencies. Yet as noted in Chapter Three, DOD leaders champion information sharing, promoting and resourcing it in anticipation other agencies will see its value and invest as well. Yet, DOD leaders struggle to define an overall role against transnational organized crime, specifically whether the role should be more active or continue in a strictly supporting capacity to federal law enforcement (and foreign partners). According to William Wechsler, a former Deputy Assistant Secretary of Defense for Counternarcotics and Global Threats, and Gary Barnabo, "it may be that DOD's role in establishing the institutional architecture that enables agencies to work together as part of a unified, whole-of-government approach is actually the most significant contribution it has made in the fight against transnational organized crime and related national security threats."[55] DOD provides the institutional architecture to match and support the whole-of-government approach of national strategy on transnational organized crime—structure follows strategy in accordance with Chandler's theory. With one sentence, Wechsler and Barnabo make a powerful argument for a proper, restrained DOD role in combating transnational organized crime and sharing information to do so.

The next chapter seeks analogous insights for solving information sharing problems from the counterterrorism arena through discussion of Joint Terrorism Task Forces, interagency fusion centers, and the National Counterterrorism Center. The intent is to identify lessons learned (or not) from counterterrorism information sharing that may assist similar efforts against transnational organized crime, including those by DOD.

---

[54] Munsing and Lamb, *Joint Interagency Task Force-South*, 69.

[55] William F. Wechsler and Gary Barnabo, "The Department of Defense's Role in Combating Transnational Organized Crime," in *Convergence: Illicit Networks and National Security in the Age of Globalization*, ed. Michael Miklaucic and Jacqueline Brewer (Washington: National Defense University Press, 2013), 240.

Chapter 5

Interagency Information Sharing for Counterterrorism

This chapter examines post-9/11 domestic counterterrorism entities with an eye toward identifying information sharing lessons learned that may assist comparable interagency efforts against transnational organized crime. Specifically, the development and growth of the Joint Terrorism Task Force (JTTF) model, interagency fusion centers, and National Counterterrorism Center (NCTC) offer strategy, structure, and culture insights that may help DOD and other relevant agencies avoid information sharing pitfalls in the fight against transnational organized crime.

The 9/11 Commission Report identified the inability to share information among law enforcement and intelligence agencies as a key failure that prevented detection and disruption of the attacks.[1] A lack of information sharing among agencies prevented development of a "coherent picture of the threats" despite production of numerous "localized snapshots" of threat information.[2] The attacks exposed "inadequate interagency coordination partially as a result of separate statutory missions and administrative barriers," identified colloquially as "stovepipes" or the "wall" between intelligence and law enforcement agencies.[3] To avoid stovepipes and break down the wall, the US Congress passed the Intelligence Reform and Terrorism Prevention Act of 2004 which mandated creation of an information sharing environment among federal organizations "to facilitate the sharing of terrorism-related information."[4] The Act encouraged JTTF expansion (the JTTF model existed since the early 1980s) and fusion center proliferation, and converted the NCTC from an initial executive-order creation into a statutory entity. Vast expansion of JTTFs, development of a National Network of Fusion Centers, and establishment of the NCTC represent significant interagency

[1] *9/11 Commission Report*, 403, 418.
[2] James Surowiecki, *The Wisdom of Crowds* (New York: Anchor Books, 2005), 69.
[3] Richard A. Best, Jr., *The National Counterterrorism Center (NCTC)—Responsibilities and Potential Congressional Concerns*, CRS Report R41022 (Washington: Congressional Research Service, 19 December 2011), 1.
[4] GAO, *Information Sharing*, 7.

developments to remedy the general failure to share information noted by the 9/11 Commission and Congress.

Joint Terrorism Task Force

A JTTF is an FBI-led interagency franchise designed to combat terrorism in the US. Its mission is "to detect and investigate terrorists and terrorist groups and prevent them from carrying out terrorist acts directed against the United States."[5] Interagency participation in JTTFs by federal, state, and local agencies serves as a "force multiplier" for FBI counterterrorism efforts, broadening informant recruiting prospects and offering combined investigative resources for collective targeting of terrorists.[6] The FBI credits JTTFs with post-9/11 success against various terrorist cells and planned attacks, including the "Lackawanna Six" (Yemeni-American al Qaeda supporters arrested in 2002), "Portland Seven" (American al Qaeda supporters arrested in 2002), and 2007 Fort Dix attack plotters.[7] Actually, the most important JTTF success is its promotion of an information sharing and interagency culture among various government levels.

As the lead federal agency for domestic terrorism investigations, the FBI expanded the number of JTTFs from 33 to 104 in the years since 9/11, including task forces in all 56 FBI field offices in major US cities and 48 other offices. A JTTF includes a mixture of federal, state, and local law enforcement and intelligence representation. The FBI boasts a four-fold increase in JTTF manpower since 9/11, with 4,000 task force members from 55 federal agencies—including DOD representation—and more than 500 state and local agencies. Moreover, the FBI views the JTTF construct as a focal point for counterterrorism information, where interagency investigators, analysts, linguists, and other specialists develop a common operating picture for terrorist threats in their area of responsibility and conduct operational and investigative activities collectively to thwart and arrest attackers. An overarching National Joint Terrorism Task Force ensures information sharing occurs among JTTFs and with external entities.[8] JTTF

[5] GAO, *Information Sharing*, 15.
[6] Department of Justice, *The Department of Justice's Terrorism Task Forces* (Washington: Office of the Inspector General, June 2005), ii-iii.
[7] Federal Bureau of Investigation, "Protecting America from Terrorist Attack: Our Joint Terrorism Task Forces," http://www.fbi.gov/about-s/investigate/terrorism/terrorism_jttfs (accessed 19 March 2015).
[8] FBI, "JTTFs," http://www.fbi.gov/about-s/investigate/terrorism/terrorism_jttfs.

representatives are also responsible for coordinating information back through their individual agency channels for awareness and appropriate action. Overall, JTTFs promote horizontal and vertical information sharing, the latter either top-down (National JTTF) or bottom-up (local JTTF representatives to parent agency headquarters).

Though a vast, highly visible example of interagency effort, the JTTF model is not above criticism. An initial critique the FBI has sought to remedy over the years is a requirement for JTTF representatives to hold security clearances. This is certainly reasonable. However, if representatives cannot share classified threat information with home agencies (e.g., state or local law enforcement) due to the absence of clearances there, then information sharing remains limited and less effective.[9] Similarly problematic, participating agencies sensed pre-9/11 that JTTF priorities were really FBI-only priorities. This de-incentivized participating agencies from providing full-time representatives, resulting in JTTF staffing shortages.[10] In essence, a *cultural* problem (FBI primacy) caused a *structural* problem (representative shortage).

Post-9/11, the huge increase in JTTFs and participating agencies indicates the FBI has addressed, to some extent, concerns over priorities. However, the nature of the lead-agency construct for JTTFs—where the FBI leads and provides basic facilities and infrastructure—may convey to participating agencies a less-than-full partnership. In fact, the proliferation of state and local fusion centers evinces a desire for a more equitable interagency arrangement with access to federal grants, but not federal leadership, as well as a broader mission beyond counterterrorism. Arguably more than FBI-led JTTFs, fusion centers provide accountable state and local governments the ability to prioritize and obtain "the right information and intelligence to enable them to potentially prevent a future attack or at least mitigate its impact and respond effectively."[11]

The fusion center critique enjoys recent support. A 2013 GAO report on information sharing notes "the FBI has several performance metrics that hold JTTFs … accountable for sharing information, but none specific to coordinating with other field-

[9] Michael German and Jay Stanley, *What's Wrong with Fusion Centers?* (New York: American Civil Liberties Union, December 2007), 6.
[10] *9/11 Commission Report*, 82.
[11] Todd Masse, Siobhan O'Neil, and John Rollins, *Fusion Centers: Issues and Options for Congress*, CRS Report RL34070 (Washington: Congressional Research Service, 6 July 2007), 18.

based entities [e.g., fusion centers, HIDTAs] in their urban areas."[12] In other words, fusion centers and other interagency entities cannot be certain FBI-led JTTFs share information fully and in accordance with their needs. In fact, post-event scrutiny of the Boston Marathon bombing investigation reveals the FBI, as late as 2013, still struggled to provide state and local JTTF representatives—let alone external entities—sufficient access to FBI information. Subsequent to the attack, the FBI sought to improve information system access and to better "facilitate the sharing of JTTF information with detailees' home agencies." In fairness, a multi-departmental inspector general report found no overall fault with the FBI or Boston JTTF's handling of a pre-bombing investigation of one of the perpetrators and concluded "that the FBI, CIA, DHS, and NCTC generally shared information and followed procedures appropriately."[13]

The JTTF model exemplifies difficulties in synchronizing strategy, structure, and culture into effective organizational outputs. The FBI and participating agencies struggle with a strategy that seeks to leverage interagency partnerships and synergies to best confront terrorism through a structure with a lead agency with its own overarching interests that may not always coincide with those of interagency partners. When this occurs, structure is out of alignment with strategy—in violation of Chandler's *structure follows strategy* thesis—and inefficiencies and ineffectiveness are more likely to appear.[14] This then has implications for the desired information sharing culture. While the FBI deserves much credit for development and expansion of the JTTF model to promote and enhance information sharing nationwide, participating agencies continue to question the FBI's commitment and motivation for information sharing. If information sharing is to become—in Schein's terms—a taken-for-granted, basic underlying assumption of a counterterrorism culture, the FBI must continue to advocate information sharing and remedy/eliminate instances where advocacy is not matched by actions, in order to convince current agencies to maintain commitments to an effective counter-

[12] GAO, *Information Sharing*, 33.
[13] Inspectors General of the Intelligence Community, Central Intelligence Agency, Department of Justice, and Department of Homeland Security, *Unclassified Summary of Information Handling and Sharing Prior to the April 15, 2013 Boston Marathon Bombings* (Washington: Intelligence Community, 10 April 2014), 10, 21.
[14] Chandler, *Strategy and Structure*, 16; Stanley Kavale, "The Connection between Strategy and Structure," *International Journal of Business and Commerce* 1, no. 6 (February 2012): 60, 69.

terrorism model and convince potential participating agencies to contribute to a valid information sharing effort.

Fusion Centers

State and local governments developed fusion centers after 9/11 to foster information sharing among multiple agencies in order to address potential criminal threats in their jurisdictions—including, but not limited to, terrorism—and respond to emergencies and disasters. In 2007, DOJ and DHS requested each state designate a fusion center as a point of contact for interaction with federal agencies, thereby solidifying the role of fusion centers in a whole-of-government approach to counterterrorism. As of June 2014, 49 states operate 78 fusion centers with significant federal grant funding augmentation.[15] DOD participation in fusion centers includes direct representation by National Guard members and indirect liaison relationships by DOD investigators. Federal funding with state or local leadership creates tension among government levels involved in fusion centers as all seek, like JTTFs, to ensure strategy, structure, and culture align to promote information sharing to defeat threats.

Federal guidance defines a fusion center as a "collaborative effort of two or more agencies that provide resources, expertise, and information to the center with the goal of maximizing their ability to detect, prevent, investigate, and respond to criminal and terrorist activity." The fusion process involves the cross-flow of information among all levels of government and the private sector in order to produce "actionable knowledge." Such knowledge requires multi-disciplinary public and private sector experts (e.g., analysts, security professionals) who exchange and analyze information to identify and address threats.[16] Cumulatively, the 78 fusion centers form the "National Network of Fusion Centers," which "connects fusion centers and strengthens national security efforts" through enhanced nationwide information sharing across agencies and interagency entities.[17] As noted in Chapter Three, the Suspicious Activity Reporting

[15] *2014-2017 National Strategy for the National Network of Fusion Centers* (Washington: Information Sharing Environment, July 2014), 1, note 1, 2.
[16] Department of Justice, *Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era* (Washington: Bureau of Justice Assistance, August 2006), 2.
[17] *2014-2017 National Strategy for the National Network of Fusion Centers*, 2.

process employed by fusion centers and other interagency entities is a positive example of multi-jurisdictional, cross-functional terrorism information sharing.[18]

Variation in fusion centers complicates federal oversight efforts to assess operations and account for grant funding, but the variation is actually a necessity and a strength of the National Network of Fusion Centers. David Carter and Jeremy Carter state, "There is no single model for a fusion center because of the diverse needs and environmental characteristics that will affect the structure, processes and products of a center." While federal officials may prefer standardization, Carter and Carter insist diversity "permits state and local agencies to mold the fusion center into a model that best suits the needs and challenges that are idiosyncratic to each jurisdiction."[19] This view conforms to Chandler's notions on the *boundaries of the firm* where proper structural alignment enables innovations that generate competitive advantages within manageable, beneficial bounds of a strategy. For fusion centers, states and localities tailor fusion centers to meet specific needs so as to best "compete" against threats and challenges unique to their jurisdictions. In addition to counterterrorism activities, fusion centers operate against an array of criminal and emergency/disaster possibilities unique to each jurisdiction. In this way, fusion centers are not only force multipliers for FBI and DHS counterterrorism efforts; they are force multipliers for DHS/Federal Emergency Management Agency (FEMA) response. Moreover, fusion centers compete in an interagency structural "marketplace of ideas," allowing for the cross-flow of information on useful structural arrangements and adoption of best practices across jurisdictions.

Undoubtedly, the federal government supports the fusion center concept as a useful way to enhance counterterrorism information sharing. Nonetheless, significant federal funding of fusion centers provides an avenue for criticism of fusion center operations. In 2014, federal grants to fusion centers—primarily FEMA non-disaster preparedness grants—totaled $73.5 million, with another $68 million in direct federal expenditures; both amounts comprise 43 percent of fusion center budgets.[20] With

---

[18] *National Strategy for Information Sharing and Safeguarding*, 4, 8.
[19] Carter and Carter, "Intelligence Fusion Process," 10-12.
[20] US House of Representatives, *Majority Staff Report on the National Network of Fusion Centers* (Washington: Committee on Homeland Security, July 2013), vi; *2014 National Network of Fusion Centers Final Report* (Washington: Information Sharing Environment, January 2015), vii.

hundreds of millions of dollars invested over the past decade, federal officials' concerns regarding return on investment appear genuine and deserve attention from fusion centers.

A 2012 US Senate bipartisan report provides harsh criticism of fusion centers and questions their value to counterterrorism efforts. Specifically, the report faults fusion centers for a lack of "reporting which uncovered a terrorist threat" or "a contribution … to disrupt an active terrorist plot."[21] In fairness, critics also question frequently whether JTTF successes are actual successes. For both JTTFs and fusion centers, it is exceedingly difficult to prove or disprove a negative, meaning these entities definitively prevented terrorist attacks. Nevertheless, the report blames DHS for failure to account for grants provided to fusion centers, including amounts, expense purposes, and funds effectiveness.[22] The GAO echoes this criticism when it states, "DHS cannot accurately account for federal funds provided to states to support these [fusion] centers."[23] The Senate report acknowledges that fusion centers are state and locally-led operations that serve purposes other than counterterrorism, but nevertheless frames its criticism as if fusion centers exist solely to support federal counterterrorism efforts.[24] This reflects a common misconception and, more importantly, a challenge for more robust use of fusion centers for other purposes—including efforts against transnational organized crime.

A 2013 US House of Representatives report on the National Network of Fusion Centers reads less harshly than the Senate report. While the House report identifies various areas for improvement, it affirms the overall value of diverse non-federal fusion centers to the whole-of-government approach to counterterrorism. The House report cites the need for federal support to improve fusion center information sharing practices, but insists responsibility for information sharing improvement lies with states and localities. Like the Senate report, the House report identifies the inability to determine the value of fusion centers to the national counterterrorism mission in relation to federal expenditures. Despite its caution against formal standardization of fusion center operations, the report

---

[21] US Senate, *Federal Support for and Involvement in State and Local Fusion Centers*, (Washington: Permanent Subcommittee on Investigations, 3 October 2012), 2.
[22] US Senate, *Fusion Centers*, 3-4.
[23] Government Accountability Office, *Information Sharing: DHS is Assessing Fusion Center Capabilities and Results, but Needs to More Accurately Account for Federal Funding Provided to Centers*, GAO-15-155 (Washington: GAO, November 2014), highlights.
[24] US Senate, *Fusion Centers*, 5.

recommends development of national and federal strategies for fusion centers to push the national network to its full potential through articulation of useful performance metrics.[25] The latter strategy has yet to appear while the former emerged in 2014.

The *2014-2017 National Strategy for the National Network of Fusion Centers* envisions "a multidisciplinary, all-crimes/all-threats/all-hazards information sharing network that protects our nation's security and the privacy, civil rights, and civil liberties of our citizens."[26] This vision statement demonstrates the disconnect of expectations between the federal government and state and local governments on the role of fusion centers, where the former views them as a funded extension of federal counterterrorism efforts and the latter views fusion centers as an independent tool to meet federal, state, and local law enforcement, disaster preparedness, and emergency management needs. The Strategy's mission statement seeks to resolve the disconnect but only adds to the expectations gap when it states fusion centers exist "to receive, analyze, disseminate, and gather threat information and intelligence in support of state, local, tribal, territorial, private sector, and federal efforts to protect the homeland from criminal activities and events, including acts of terrorism."[27] Fusion centers are the states' information sharing contribution to homeland security, a broader concept that includes, but is not limited to, counterterrorism. It is important to recognize that state, local, and federal officials participated in the crafting of this strategy document. The Strategy is a significant step to establish clearly the roles and responsibilities of fusion centers. It offers a way to assess and account for fusion center resource usage and provides near-term goals and objectives to improve fusion center capabilities and outputs.

Prior to this strategy document, and despite general references to fusion centers in other strategy documents, fusion centers represented a structural and cultural tool to improve information sharing on terrorist activities *without a specific guiding strategy*. The evolution and debate over fusion centers demonstrate the necessity for a synergistic combination of strategy, structure, and culture to express, organize, and fulfill enterprise purposes. With a national strategy, fusion centers now have specific direction and focus

[25] US House of Representatives, *National Network of Fusion Centers*, iv-v.
[26] *2014-2017 National Strategy for the National Network of Fusion Centers*, 7.
[27] *2014-2017 National Strategy for the National Network of Fusion Centers*, 7.

to guide their unique structures, fulfilling Chandler's intent for a firm or enterprise.[28] Moreover, fusion centers epitomize interagency information sharing. Unquestionably, information sharing is a basic underlying assumption for fusion center culture. Fusion centers recognize and promote information sharing as "valid and, therefore, to be taught to new members as the correct way to perceive, think, and feel" in conducting their all-crimes/all-threats/all-hazards mission.[29] Overall, the National Network of Fusion Centers possesses a strategy, tailored structures, and a committed information sharing culture. The continuing challenge for fusion centers is to enhance each of these areas and, more specifically, to clarify and improve an enduring relationship with the federal government through demonstrated and recognized value.

National Counterterrorism Center

Based on a 9/11 Commission recommendation, President George W. Bush established the NCTC in 2004 by executive order; subsequently, the Intelligence Reform and Terrorism Prevention Act of 2004 codified the NCTC as an entity. The NCTC is a "central and shared knowledge bank on terrorism information" that "provides all-source intelligence support to government-wide counterterrorism activities."[30] Perry labels the NCTC a "Federal Fusion Center" for integration and analysis of terrorism and counterterrorism intelligence.[31] The NCTC includes representatives from across the Intelligence Community, including DOD. As an intelligence entity, the NCTC reports to the Director of National Intelligence, but in a unique, challenging dual-reporting chain, reports to the President regarding federal counterterrorism planning.[32]

The NCTC mission is to "lead our nation's effort to combat terrorism at home and abroad by analyzing the threat, sharing information with our partners, and integrating all instruments of power to ensure unity of effort."[33] While the latter phrase recognizes the whole-of-government approach of the *National Security Strategy*, information sharing is

---

[28] Chandler, *Strategy and Structure*, 13-14.
[29] Schein, *Organizational Culture and Leadership*, 18.
[30] National Counterterrorism Center, "Who We Are," http://www.nctc.gov/whoweare.html (accessed 21 March 2015).
[31] Perry, "Information Sharing," 10.
[32] National Counterterrorism Center, "Overview," http://www.nctc.gov/overview.html (accessed 21 March 2015).
[33] *2013-2015 National Counterterrorism Center Strategic Intent* (Washington: National Counterterrorism Center, October 2012), 3.

central to NCTC's mission and vision to "serve as the nation's indispensable source for counterterrorism analysis and strategic operational plans."[34] The NCTC must obtain and share information in order to conduct effective, all-source analysis. In this endeavor, the NCTC leverages access to over 30 network systems with over 80 data sources, including intelligence, law enforcement, military, and homeland security.[35] The NCTC accesses information from diverse sources but also provides information from several internal databases. The Terrorist Identities Datamart Environment (TIDE) system supports screening and watchlisting for suspected terrorists, while two classified systems—NCTC Online and NCTC Online CURRENT—share NCTC products with 75 agencies across the US government. The NCTC also hosts an Interagency Threat Assessment and Coordination Group to promote counterterrorism information sharing among the Intelligence Community and federal, state, and local law enforcement agencies. Overall, the strategy, structure, and culture at work in the NCTC appear to lend credence to its self-proclamation as a "model of interagency information sharing."[36]

Yet, like JTTFs and fusion centers, the NCTC is not above criticism, even from one of its own. Its former director insists the organization must "advance our business practices to improve NCTC's culture of collaboration, communication, and integrity; and improve our use of information technology resources to strengthen our core capabilities."[37] Writing in 2007 at the US Army War College, Brian Reinwald argues the NCTC is not meeting its full potential due to a lack of resources and authorities; as a result, it is neither effective nor efficient and fails to meet Congressional intent. He faults the NCTC for "a seeming unwillingness to take a bold implementation approach and a preference to avoid bureaucratic conflict."[38] Reinwald also questions the NCTC's hybrid manning construct (a mix of permanent employees and rotational agency detailees),

---

[34] *2013-2015 National Counterterrorism Center Strategic Intent*, 3.
[35] Mike McConnell, "Overhauling Intelligence," *Foreign Affairs* 86, no. 4 (July/August 2007): 54; NCTC, "Overview," http://www.nctc.gov/overview.html.
[36] NCTC, "Overview," http://www.nctc.gov/overview.html.
[37] Matthew G. Olsen, "From the Director," in *2013-2015 National Counterterrorism Center Strategic Intent*, 2.
[38] Brian R. Reinwald, "Assessing the National Counterterrorism Center's Effectiveness in the Global War on Terror" (Master's thesis, US Army War College, 6 March 2007), 1, 8.

warning it "sustains an environment that fosters continued loyalty of NCTC employees to their parent agencies rather than the NCTC itself."[39]

A 2011 Congressional Research Service report asserts the NCTC missed opportunities to detect and thwart the failed "underwear bomber" in his attempt to blow up a Detroit-bound flight on Christmas Day 2009. In fact, the report quotes President Obama, who stated, "This was not a failure to collect intelligence; it was a failure to integrate and understand the intelligence that we already had."[40] Is this not a direct condemnation of the NCTC mission? Likewise, the US Senate Select Committee on Intelligence concluded the NCTC failed to connect reporting on the attempted bomber and failed to watchlist him. The episode exposed that "the NCTC was not organized adequately to fulfil its mission," and, despite the existence of the NCTC, "no one agency saw itself as being responsible for tracking and identifying all terrorism threats."[41] Of course, it is unfair to condemn one entity out of many for one intelligence failure; hence, the Senate spreads the blame among various parties. Yet scrutiny of the underwear bomber episode demonstrates that humility is appropriate for any entity charged with detection of threats. As adversaries continue to find ways to attack the US, counterterrorism entities must refine their strategies, structures, and cultures continually to keep pace—and respond to second-guessing in the aftermath of failures with meaningful and useful reforms. To do so, counterterrorism leaders must foster an agile mindset throughout their organizations in order to produce innovations that provide competitive advantages over foes in an ever-evolving threat context.

The NCTC represents a combination of strategy, structure, and culture in a federal interagency construct dedicated to information sharing in the counterterrorism enterprise. The NCTC strategy and structure appear internally consistent; direction and focus align with resources to provide a national terrorism knowledge bank and analytical fusion center. However, aforementioned criticism reflects doubts as to whether NCTC strategy

[39] Reinwald, "Assessing the National Counterterrorism Center," 9.
[40] President Barack Obama, "The Urgency of Getting This Right," 5 January 2010, in Best, *The National Counterterrorism Center,* 1.
[41] US Senate, *Unclassified Executive Summary of the Committee Report on the Attempted Terrorist Attack on Northwest Airlines Flight 253* (Washington: Select Committee on Intelligence, 18 May 2010), 1-2.

and structure meet Congressional intent or public expectations. Is the NCTC rising to its full potential? This is unclear. Congress and the president must clarify the intent for the NCTC and NCTC leadership should aggressively seek to meet the clarified intent. On the positive side, as with fusion centers, information sharing is a basic underlying assumption of NCTC culture—a taken-for-granted *raison d'etre*. The issue is whether NCTC should be an enforcer of information sharing, or simply exist as another information repository that agencies contact on an as-needed basis. Again, intent is key to assessment and potential adjustment of the NCTC's information sharing culture.

Information Sharing Insights from Counterterrorism

Strategy, structure, and culture for information sharing in counterterrorism efforts remain works in progress, as exemplified by the evolution and issues of JTTFs, fusion centers, and the NCTC. The emphasis on information sharing, and promotion of a cultural mindset to do so, in the post-9/11 law enforcement and intelligence agency environment is clear. In line with a national whole-of-government strategic approach, all governmental levels in the US continue to refine interagency strategies and constructs to achieve the cultural vision of efficacious information sharing to defeat terrorist threats. This goal applies equally to efforts against transnational organized crime. Moreover, the post-9/11 experiences of JTTFs, fusion centers, and the NCTC provide several useful insights for DOD and other agencies to apply to information sharing for efforts against transnational organized crime.

A JTTF is a highly visible example of interagency information sharing. As a key tool in FBI efforts against its top priority, JTTFs evolved after 9/11 into a valuable, effective entity leveraging collective law enforcement and intelligence resources to detect, prevent, or react to terrorist attacks. Yet, the JTTF model is by no means perfect. Like SOD and EPIC, the JTTF model demonstrates the weakness of the lead-agency construct. Arguably an imbalanced interagency entity, it is weighted toward the interests and priorities of the lead agency, in this case, the FBI. An ideal interagency construct is a partnership, with equal status—if not equal resources—contributed by each partner agency, as found in JIATFS and NCTC. A construct where participating agencies may question lead agency priorities and candor as to information relevant to the interagency

effort is not ideal and poses a risk for potential ineffectiveness due to resource fragility (i.e., agencies can recall detailed personnel) and mistrust.

Nevertheless, the JTTF model demonstrates that a large, tradition-bound bureaucratic organization like the FBI (or DOD) can promote culture change, from a mindset of information hoarding to information sharing, in an impressive and effective way. The JTTF model promotes information sharing benefits to other internal FBI mission areas (e.g., organized crime) and externally to valued partner agencies who witness information sharing benefits and may reform their own strategies, structures, and cultures to reap similar benefits, best exemplified by the advent of fusion centers.

Like JTTFs, the post-9/11 proliferation of state and local fusion centers shows an information sharing culture is spreading and taking hold across the nation, and indicates the interagency construct is an effective means to enforce and promote sharing for matters of interest at various government levels and functions (including the military). A key lesson from the evolution of fusion centers into a national network is that funding and interests must align. If the federal government intends fusion centers to be counterterrorism-only entities, it should allocate funds to the states with explicit guidance and incentives that reflect its intent clearly. Instead, some Congressional auditors complain fusion centers misuse federal funding when monies are not used specifically for counterterrorism. This criticism ignores the fact that the majority of allocated federal funds are FEMA grants, monies appropriate for emergency management which is a legitimate mission area for fusion centers. It also ignores the likelihood that state fusion centers would continue to operate as all-crimes/all-threats/all-hazards interagency entities in the absence of federal funding, albeit with reduced resources and capabilities.[42]

Another key insight for fusion centers is that they are typically oriented to analysis; any operational role is at best limited to emergency response, not interdiction or investigation. Fusion centers feed analytical products, intelligence, and information to operational authorities via representatives and liaison networks for appropriate action. Leaders at all levels should recognize fusion centers are not "one-stop shops." However, they are an important multi-use, multi-directional information conduit. It is important to note the current and potential value fusion centers hold for efforts against transnational

[42] US House of Representatives, *National Network of Fusion Centers*, vi.

organized crime. In fact, in a 2014 report, 57 of 78 fusion centers cited transnational organized crime as a specific mission focus area in 2014, a 24 percent increase from 2013.[43] This trend indicates fusion centers recognize transnational organized crime as a threat to state and local jurisdictions, worthy of attention and resources. The flexibility inherent in the fusion center construct allows jurisdictions to alter mission priorities and innovate in terms of structure and culture to meet an evolving threat environment.

Overall, fusion centers represent American federalism at work. Armed now with a national strategy that promotes an information sharing culture (as well as improved accountability for funding at all levels), state and local governments continue to tailor fusion center structures to meet the unique demands of each jurisdiction. The National Network of Fusion Centers represents numerous laboratories where individual fusion centers can experiment and adapt over time to meet new threats; other fusion centers can choose to imitate beneficial adaptations that align with their jurisdictional needs. The lack of standardization adds complexity to the network and challenges federal oversight, but allows for flexibility and innovation that standardization tends to suppress.

Arguably a federal fusion center, the NCTC came into being as a direct result of the 9/11 attacks. It represents the priority given to the counterterrorism mission by the US government in response to the attacks, including an emphasis on interagency coordination and information sharing. However, the NCTC's evolution offers a lesson in expectations management. Simply labeling an entity as "national" does not confer automatic deference and respect from other entities and agencies, nor does "counterterrorism" mean the NCTC is equipped with authorities and resources to confront terrorism fully on its own. The NCTC competes with the Counterterrorism Center of the Central Intelligence Agency, as well as the JTTFs, FBI, DHS, DOD, National Network of Fusion Centers, etc., for relevance in terms of useful information and intelligence on terrorist threats.[44] Like fusion centers, the NCTC is an "information clearinghouse," an analytical entity lacking operational authorities or resources.[45] It relies on other entities (e.g., JTTFs, FBI, DHS, DOD) to conduct operations or

[43] *2014 National Network of Fusion Centers Final Report*, 9-10.
[44] Best, *The National Counterterrorism Center*, 1, 5, 10.
[45] Carter and Carter, "Intelligence Fusion Process," 28.

investigations to thwart or apprehend terrorists but lacks the authority to compel them to do so. The name "National Counterterrorism Center" conveys to Congress and the general public that the NCTC is the primary entity responsible for protecting the homeland from terrorist attacks, when it is not charged or resourced to do so—at least not alone. The NCTC is one of many organizations throughout all levels of government in the US involved in the counterterrorism fight. The US government and general public may feel good knowing the NCTC exists but should recognize and understand what it exists to do and the limitations of its mission and capabilities. As part of the NCTC, the DOD in particular should recognize the entity's limits and avoid overreliance on its capabilities, but DOD should also seek to augment NCTC capabilities as appropriate with resource and infrastructure support to help the entity achieve its full potential.

Postured to confront threats, JTTFs, fusion centers, and the NCTC represent strategies and structures with energetic information sharing cultures. These entities demonstrate the US government has made substantial progress in promoting and establishing an information sharing culture throughout the counterterrorism enterprise. Still, JTTFs, fusion centers, and the NCTC remain works in progress, constantly in pursuit of strategy, structure, and culture refinements to enhance mission effectiveness. The US House of Representatives notes five significant post-9/11 attacks on the homeland as deadly reasons to press for further improvements to the counterterrorism enterprise. The House report states, "We have come to understand that homeland security, including counterterrorism efforts, must be a National responsibility – a true and equal partnership across all levels of government [including DOD], and inclusive of the American people."[46] This is a powerful endorsement of the interagency construct to promote information sharing for counterterrorism efforts. Interestingly, beyond military, intelligence, and law enforcement organizations, inclusion of the American people in this statement assigns a level of responsibility for preventing attacks to individual American citizens, and presumably private sector firms as well.

[46] US House of Representatives, *National Network of Fusion Centers*, iii, which cites five post-9/11 US homeland attacks as follows: "the Little Rock Recruiting Station shooting (2009); the Fort Hood shooting (2009); the attempted bombing of Northwest Airlines Flight 253 on Christmas Day (2009); the attempted car bombing in Times Square (2010), and the Boston Marathon bombings (2013)."

It also prompts acknowledgement of a growing concern for Americans as to the proper balance between security and privacy. Despite limitations and issues noted in this chapter, JTTFs, fusion centers, and the NCTC possess significant actual and latent power to accumulate and disseminate vast amounts of information on American citizens, whether acquired through law enforcement or intelligence channels. Americans are well within their rights to question if these entities and others involved in the counterterrorism enterprise are empowered fully to confront terrorist dangers while avoiding the danger of eroding cherished civil rights and liberties—in essence, providing a form of victory to terrorists. Likewise, privacy considerations must be part of any discussion for crafting and refining an enterprise that shares information on transnational organized crime threats effectively; otherwise, Americans will trade one societal ill for another.

Mindful of the dangers of mission creep, JTTFs, fusion centers, and the NCTC also represent existing means the US government can leverage for use against transnational organized crime (at least when a terrorist nexus exists), or templates for similar new entities in the transnational organized crime fight. Either way, an information sharing culture is an accepted norm and value that organizational leaders should establish and refine continually to ensure success. Moreover, crafters of future strategies, structures, and cultures to confront transnational organized crime should be mindful that stovepipes or walls may exist in different forms than that which prompted the emphasis on information sharing originally after 9/11. Richard Best asserts, "The most important 'wall' may not be the one that existed between law enforcement and intelligence agencies prior to 2001, but the one that often persists between analysts and operators."[47] DOD and other agencies would be wise to understand and account for this dynamic—and other information sharing insights noted in this chapter—in perfecting the enterprise against transnational organized crime.

[47] Best, *The National Counterterrorism Center*, 10.

Chapter 6

Conclusion: Key Findings and Recommendations

This final chapter reviews key findings from the analysis of strategy, structure, and culture in relation to information sharing in US efforts to combat transnational organized crime, as well as analysis of information sharing by US counterterrorism entities. Recommendations stem from the study's findings and seek to improve information sharing in terms of strategy, structure, and culture. More specifically, the recommendations offer the US government in general and DOD in particular options to consider to posture resources to obtain and share information related to transnational organized crime more effectively for exploitation. First, it is important to restate the rationale and framework used to guide this study's analysis.

Transnational organized crime matters. Transnational criminal organizations continue to accumulate unprecedented illegal monetary gains at the expense of licit trade. They continue to expand negative influential power, with detrimental political and societal effects in developed and developing states. Ties among criminal, terrorist, or insurgent organizations provide a rationale to treat transnational criminal activities as national security threats, not solely law enforcement matters. Still, it is important not to press the notion of a "crime-terror-insurgency nexus" too far. Transnational organized crime represents a national security threat and deserves attention due to the scale and scope of the problem—even without any actual links to terrorism or insurgency.

Information sharing on transnational organized crime threats matters. A major challenge in confronting the transnational organized crime threat is to share information on diverse actors and activities to enable relevant agencies to pursue suitable measures in a timely manner. Unfortunately, despite a significant cultural shift on information sharing throughout the US government, impediments (i.e., stove-piping, information hoarding as agency leverage) persist over a decade after acknowledged information sharing failures surrounding the 9/11 attacks. Transnational organized crime cuts across borders and jurisdictions, and encompasses a variety of crimes of an enduring nature. Without efficacious information sharing, efforts against transnational organized crime

will suffer from lack of coordination, blunting the potential collective impact of substantial US government capabilities against a national security threat.

The US government must synchronize strategy, structure, and culture in order to solve information sharing problems with efforts to combat transnational organized crime. Specifically, the US government should leverage lessons learned from counterterrorism efforts to improve information sharing in that area, but leaders and members of relevant organizations must recognize both similarities and differences between efforts against transnational organized crime and terrorism. Since legal, operational, technological, bureaucratic, and cultural frictions impede ideal information sharing, responsible entities within the US government, including DOD, must comprehend and navigate these issues in order to posture resources effectively to obtain and share information related to transnational organized crime for exploitation by appropriate authorities.

This study used a strategy/structure/culture framework to identify information sharing issues and problems requiring remedies to enhance US government efforts against transnational organize crime. Chandler's notions of *strategy* and *structure* assisted analysis of key US strategy documents on transnational organized crime and information sharing and relevant institutions and processes. Specifically, this study used Chandler's thesis that *structure follows strategy* to determine if institutions and processes match strategies to produce effective information sharing on transnational organized crime. Schein's *organizational culture* model complements Chandler's ideas and serves to bind strategy and structure together; therefore, this study leveraged Schein's model to assess whether relevant US government strategies and structures promote an effective information sharing culture to fight transnational organized crime. The framework also assisted analysis of post-9/11 US counterterrorism efforts to discover useful insights for information sharing applicable to the fight against transnational organized crime.

Key Findings

Strategy and Culture: Information Sharing on Transnational Organized Crime. Using Chandler and Schein's respective notions of strategy and organizational culture, analysis revealed that select US strategy documents represent a cumulative good-faith effort to provide direction, guidance, and prioritization of effort for the US government—including DOD—toward a shared goal to improve information sharing on transnational

organized crime. However, several problems and inconsistencies within the strategy documents may cause difficulties in policy implementation and execution.

One overarching challenge in promoting change of any sort is how to co-opt others so they view change as positive, possible, and worthy of supporting efforts. To enhance information sharing on transnational organized crime, an incentive area may lie in convincing agencies of high rewards for dismantling large, complex, powerful, negative-influencing organizations, and actually following through with the rewards (e.g., promotions, recognition, budget increases). There is certainly more room to consider providing organizations with incentives to embrace information sharing as not only an intrinsically good idea, but a practical way to enhance counter-threat activities. A related challenge is how to enforce discipline in those instances when information is not shared when it should be or is provided improperly in a less than secure manner. To build a culture of trust that promotes information sharing requires construction of rules, rewards, and punishments applicable to individuals in multiple peer organizations.

Currently, DOD is uncertain as to its proper role in efforts against transnational organized crime and approaches change in this area cautiously. While its strategy documents advocate strongly for information sharing, DOD accords transnational organized crime varying levels of attention. Transnational organized crime's uncertain value to DOD likely stems more from the "crime" element of the phenomenon than the "transnational" security threat element, since federal law restricts military involvement in strictly law enforcement matters. Nonetheless, DOD must find a cultural comfort zone where it accepts a general supporting role in the fight against transnational organized crime—including active information sharing on threats and facilitation of sharing—while it also seeks sufficient latitude in authorities to bring unrivaled capabilities to bear more fully in specific instances against a threat deemed significant by national leaders.

Structure and Culture: Information Sharing on Transnational Organized Crime. Leveraging Chandler and Schein's respective notions on structure and culture, analysis sought to determine if US government structures follow strategy documents in promoting effective information sharing on transnational organized crime. This study examined key US structures involved in efforts against transnational organized crime: Special Operations Division, El Paso Intelligence Center, and Joint Interagency Task Force

South. These entities represent different interagency models for lines of authority and communication, and their functions also vary. A diversity of interagency models and functions is an advantage, not a weakness. While minimizing duplicative efforts, it is valuable for entities to develop niche capabilities and to compete and adapt based on other entities' successes and failures in order to enhance overall efforts against transnational organized crime threats.

It appears SOD, EPIC, and JIATFS embrace the benefits of information sharing and interagency cooperation to confront threats, which may reflect entrenchment of post-9/11 cultural shifts based on counterterrorism lessons learned. Interagency entities also pursue organizational changes to adapt to dynamic threats, expanding abilities to address a wider range of transnational organized crime. Flexibility in capabilities and authorities is a positive attribute for interagency entities. However, the potential pitfall here is mission creep, with entities chasing continued relevance through broadened missions against the full range of transnational organized crime threats. The US government should continue to fund and promote a diverse array of entities working against different aspects of the complex transnational organized crime phenomenon.

Overall, analysis revealed both successes and challenges in translating strategy on transnational organized crime and information sharing into structures that conduct activities in accordance with strategic direction. The current cumulative structural arrangement meets the intent of the whole-of-government approach in the *Strategy to Combat Transnational Organized Crime*. A relatively horizontal, diffuse network of interagency entities shares information across entities to combat transnational organized crime networks, and works continually to refine information sharing and cooperation with combined resources. Since individual agencies retain their independence and unique authorities and capabilities while cooperating with interagency entities, the arrangement also remains true to the spirit and intent of separation of powers in the US Constitution. Properly in line with American cultural values, the US government continues to promote cooperation—not consolidation—of powers to address threats.

DOD's leaders champion information sharing—promoting and resourcing information sharing in anticipation other agencies will recognize value in doing so and invest as well. Yet, as with strategy so it is with structure, DOD leaders struggle to

define an overall role against transnational organized crime, specifically whether the role should be more active or continue in a strictly supporting capacity to federal law enforcement (and foreign partners). Fortunately, as Wechsler and Barnabo state, "It may be that DOD's role in establishing the institutional architecture that enables agencies to work together as part of a unified, whole of government approach is actually the most significant contribution it has made in the fight against transnational organized crime and related national security threats," which is a powerful argument for a proper, restrained DOD role in combating transnational organized crime and sharing information to do so.[1]

Information Sharing Insights from Counterterrorism. Analysis of post-911 US counterterrorism efforts afforded an opportunity to discover useful insights for information sharing applicable to the fight against transnational organized crime. Mindful of the dangers of mission creep, Joint Terrorism Task Forces, fusion centers, and the National Counterterrorism Center represent existing means the US government can leverage for use against transnational organized crime (at least when a terrorist nexus exists), or at least templates for similar entities in the transnational organized crime fight.

The development and growth of the JTTF model, interagency fusion centers, and NCTC offer strategy, structure, and culture lessons that may help DOD and other relevant agencies avoid information sharing pitfalls in the fight against transnational organized crime. However, analysis revealed strategy, structure, and culture for information sharing in counterterrorism efforts remain works in progress, as exemplified by the evolution and issues of JTTFs, fusion centers, and the NCTC. Like SOD and EPIC, the JTTF model demonstrates the weakness of the lead-agency construct. A positive example for DOD, the JTTF model demonstrates that a large, tradition-bound bureaucratic organization like the FBI can promote effective culture change, from a mindset of information hoarding to information sharing. A key lesson from the evolution of fusion centers into a national network is that funding and interests must align. Another key insight for fusion centers is that they are typically oriented to analysis; any operational role is at best limited to emergency response, not interdiction or investigation. A lack of standardization adds complexity to the fusion center network and challenges

[1] Wechsler and Barnabo, "The Department of Defense's Role in Combating Transnational Organized Crime," 240.

federal oversight, but allows for flexibility and innovation that standardization tends to suppress. For the NCTC, its evolution offers a lesson in expectations management. The US government and general public should understand what the NCTC exists to do and the limitations of its mission and capabilities. The NCTC is an analytical entity lacking operational authorities or resources. It is not the primary entity responsible for protecting the homeland from terrorist attacks, nor is it charged or resourced to do so.

Despite noted limitations and issues, JTTFs, fusion centers, and the NCTC possess significant actual and latent power to accumulate and disseminate vast amounts of information on American citizens, whether acquired through law enforcement or intelligence channels. In line with debates regarding the proper balance between security and freedom in counterterrorism efforts, civil rights and liberties considerations (e.g., privacy) must be part of any discussion for shaping and refining an enterprise that shares information on transnational organized crime threats.

Overall, JTTFs, fusion centers, and the NCTC represent strategies and structures prepared to confront threats with energetic information sharing cultures. Analysis of these entities shows the US government has made substantial progress in establishing an information sharing culture throughout the counterterrorism enterprise. The emphasis on information sharing, and promotion of a cultural mindset, in the post-9/11 law enforcement and intelligence agency environment is clear. In line with a national whole-of-government strategic approach, all governmental levels in the US continue to refine interagency strategies and constructs to achieve the cultural vision of efficacious information sharing to defeat terrorist threats.

Recommendations

Option 1: The US improves its existing strategy, structure, and culture to enhance information sharing for a decentralized enterprise against transnational organized crime. To improve strategy for the existing decentralized enterprise, the US Congress should provide a statutory definition for transnational organized crime. Current US definitions of transnational organized crime are policy statements, subject to change by subsequent administrations, lacking the force or endurance of federal law. Though enabling flexibility to adapt to evolving threats at a policy level, the lack of a legal definition and statutory roles and responsibilities approved by Congress creates long-term

planning, resourcing, and accountability issues for entities, including DOD, that fight transnational organized crime. A statutory definition of transnational organized crime will help alleviate these types of issues by providing an enduring, unifying anchor on which to focus efforts. Moreover, a definition enhances information sharing by providing accepted boundaries for what is and what is not transnational organized criminal activity.

It is also important that the legislative and executive branches *not* identify a lead federal agency or department for transnational organized crime investigations. A decentralized approach offers the best opportunities for experimentation and beneficial competition among different information sharing models to innovate capabilities and processes to tackle transnational organize crime more effectively. SOD, EPIC, JIATFS (and other JIATFs), JTTFs, fusion centers, and the NCTC—as well as other relevant US entities and agencies—represent existing structures that, empowered with requisite statutory authorities, can engage transnational organized crime threats collectively, sharing information to do so effectively in a decentralized way. Additionally, in those instances when transnational organized crime and terrorist threats commingle, terrorism-focused entities already possess authorities and capabilities to respond.

An information sharing culture has taken root at all levels of government in the US; to continue to flourish, the information sharing culture requires continual enhancement to ensure the decentralized approach functions properly and effectively. Congress incentivizes information sharing at the federal level through the "power of the purse," using budgetary discretion to reward or punish information sharing behaviors by agencies and departments. Congress influences information sharing behaviors at the state and local levels in much the same way, offering or withholding federal grant monies for fusion centers based on information sharing performance across levels of government and jurisdictions. One caveat is in order: Congress and the American public should understand that information sharing among agencies and levels of government should never be "easy." The Constitution and federalism demand separation of powers, which prevents complete centralization of authority and information in one entity. Meanwhile, civil rights and liberties insist on a balance between information sharing *and* safeguarding to prevent government encroachments on privacy, expression, and other sacred freedoms.

Within a decentralized approach, DOD must recognize transnational organized crime as a national security threat and embrace a supporting role throughout various strategy documents. DOD should continue its laudable promotion of information sharing and offer assistance through existing structures in which it participates, including extensive capabilities to share information. Yet, DOD must guard against any perceptions it enforces civilian laws or infringes on civil rights and liberties in any way (or encourages others to do so). Efforts against transnational organized crime as a national security threat need not lead to militarization of the enterprise. This is unnecessary and unwise, for the foregoing reasons as well as to avoid mission creep, as DOD must prepare to deter and defeat other threats that require a military response.

Transnational organized crime indeed poses a national security threat, but it is incomparable to other national security threats that may pose an existential threat (e.g., weapons of mass destruction proliferation, nuclear conflict). Therefore, a decentralized approach strikes the proper balance between addressing the threat and adhering to the Constitutional principles of American federalism, checks and balances, and separation of powers. A transnational criminal organization is unlikely to conduct acts that cause a catastrophic event (e.g., Pearl Harbor, 9/11), despite fears by those concerned with a crime-terror nexus. This is so due to incompatible motives: criminals pursue illicit profits at the expense of an existing politico-economic system—without threatening the system or drawing publicity—and terrorists perpetrate high-publicity political violence to advance an ideology to the detriment of an existing system.

Option 2: If forced by a catastrophic event, the US creates an integrated, operational task force for homeland protection against transnational organized crime. Future events are inherently unpredictable; therefore, the possibility of a transnational organized crime-related catastrophic event exists. Potential examples include an unprecedented simultaneous cyber-theft of multiple US financial institutions (i.e., the largest bank robbery of all time) that empties the bank accounts of millions of Americans, or an uncontrollable wave of cross-border killings and kidnappings in the southwest US involving rival transnational criminal organizations that overwhelms law enforcement capabilities to stop the violence. Or, worst case, if a transnational criminal organization facilitates the entry of a weapon of mass destruction that detonates in a US city and

causes large numbers of casualties, political leaders will face an impossible-to-ignore public demand to change the government's handling of transnational organized crime. Considering these possibilities, it is irresponsible to consider only a status quo-friendly recommendation to enhance efforts against transnational organized crime.

If an event forces politicians to "do something" different regarding transnational organized crime, US strategy will most likely turn more aggressive against the threat. Demands for increased abilities to "connect the dots" for transnational organized crime threats will prompt calls for streamlined information sharing processes, perhaps to the detriment of calls for preservation of strict safeguards for classified and privacy information. All of this should sound familiar based on post-9/11 US political reactions.

The real change politicians should consider in the aftermath of a catastrophic transnational organized crime-related event is structural: an integrated, operational task force—a "JIATF-TOC"—for homeland protection against transnational organized crime.[2] As evidenced by the success of JIATFS against drug trafficking organizations, an interagency construct with true partnerships among contributing agencies, empowered for analytical fusion and operational tasks, can succeed against transnational organized crime threats. In fact, JIATF-TOC could come into being by expanding the roles, responsibilities, and resources of JIATFS (perhaps maintaining a subordinate task force committed exclusively to the previous, highly effective JIATFS mission) and incorporating the mission of Joint Task Force North, which supports federal law enforcement agencies operating along the Southwest border against transnational criminal organizations. Based on the homeland security aspect of a transnational organized crime-related catastrophic event as an impetus for change, the Congress should designate DHS as the overall lead department for transnational organized crime, responsible to the National Security Council for operational coordination and information sharing across federal entities and among levels of US government (unfortunately, the benefits of a decentralized approach bend to fears of another catastrophic event, prompting a centralized reaction). Based on the government-wide respect and trust in the

[2] The notion of a "JIATF-TOC" owes its origin to Matthew McDonald's advocacy for creation of a "JIATF-Illicit Trafficking" with jurisdiction along the Southwest border of the US. See McDonald, "Joint Interagency Task Force-Illicit Trafficking," 22-25.

US Coast Guard, and the maritime service's proven ability to balance and leverage its military and law enforcement authorities, a Coast Guard flag officer should lead JIATF-TOC, with a DEA or other DOJ senior representative as deputy director.

In a more centralized approach prompted by a catastrophic event, DOD would no doubt recognize transnational organized crime as a national security threat and embrace a supporting role throughout various strategy documents. As with JIATFS, DOD's proper role would be to provide supporting infrastructure— including backbone infrastructure to facilitate information sharing—and military capabilities as needed to confront transnational organized crime, within the bounds of *Posse Comitatus*. The difficulty for DOD would be to restrain inclinations for a more active role in an essentially homeland security-driven enterprise. In Chandlerian terms, DOD must avoid over-extending its boundaries of the firm into mission areas for which it is not fully authorized to operate and does not possess a competitive advantage vis-à-vis US law enforcement and homeland security agencies. Of course, DOD military resources will be used abroad as deemed appropriate by political leaders to engage and preempt time-sensitive threats. Yet, "political sensitivities and rules of engagement may prevent or prohibit the U.S. Armed Forces from direct involvement" and "may risk escalating suppression tactics and contribute to violations of human rights."[3]

Ultimately, regardless of the option chosen, the US must not sacrifice its character in the face of transnational organized crime threats, whether the value is a commitment to a separation between law enforcement and military activities, respect for sovereignty, protection of civil rights and liberties, the principles of federalism, separation of powers, checks and balances, and the rule of law, or belief in the benefits of competition and innovation. To sacrifice such values to counter threats merely trades one evil for another.

To achieve the goal of improving information sharing on transnational organized crime requires strategies and plans that provide clear direction, useful guidance, and prioritization of effort. To translate strategies into reality requires proper structures to conduct activities in accordance with strategic direction. Solutions to information sharing

[3] John Rollins and Liana Sun Wyler, *Terrorism and Transnational Crime: Foreign Policy Issues for Congress*, CRS Report R41004 (Washington: Congressional Research Service, 11 June 2013), 26.

problems with transnational organized crime lie in ensuring the presence of sound strategy, effective structures to implement the strategy, and organizational cultures that embrace the strategy and fully leverage structural resources to achieve strategic goals. Where these elements are identified as lacking or missing is where the need for improvement exists, and identification of problems is the first step toward improvement. Hopefully, this study assists and adds to others' efforts to identify problems and offer solutions to improve information sharing on transnational organized crime in order to help DOD and the US government to fight this scourge more effectively and reduce its impact on society—from a significant threat to a tolerable nuisance.

ACRONYM LIST

ATF	Bureau of Alcohol, Tobacco, Firearms and Explosives
BIFS	Border Intelligence Fusion Section
CBP	Customs and Border Protection
CIA	Central Intelligence Agency
CJCS	Chairman of the Joint Chiefs of Staff
CRS	Congressional Research Service
DASD	Deputy Assistant Secretary of Defense
DEA	Drug Enforcement Administration
DEC	Digital Equipment Corporation
DHS	Department of Homeland Security
DOD	Department of Defense
DODD	Department of Defense Directive
DOJ	Department of Justice
EPIC	El Paso Intelligence Center
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
GAO	Government Accountability Office
HIDTA	High Intensity Drug Trafficking Area
IC	Intelligence Community
ICE	Immigrations and Customs Enforcement
IG	Inspector General
IPC	Interagency Policy Committee

JIATFS	Joint Interagency Task Force South
JIATF-TOC	Joint Interagency Task Force-Transnational Organized Crime
JTTF	Joint Terrorism Task Force
NCTC	National Counterterrorism Center
NMS	*National Military Strategy*
NSS	*National Security Strategy*
ONDCP	Office of National Drug Control Policy
SOD	Special Operations Division
TCO	Transnational Criminal Organization
TIDE	Terrorist Identities Datamart Environment
TOC	Transnational Organized Crime
UN	United Nations
UNODC	UN Office on Drugs and Crime
US	United States

BIBLIOGRAPHY

Academic Papers

Bucheli, Marcelo, Joseph T. Mahoney, and Paul M. Vaaler. "Chandler's Living History: The Visible Hand of Vertical Integration in 19th Century America Viewed Under a 21st Century Transaction Costs Economics Lens." Champaign: University of Illinois at Urbana-Champaign, 2007, http://www.business.uiuc.edu/Working_Papers/papers/07−0111.pdf.

Chau, Michael, Homa Atabakhsh, Daniel Zeng, and Hsinchun Chen. "Building an Infrastructure for Law Enforcement Information Sharing and Collaboration: Design Issues and Challenges." Tucson: University of Arizona Campus Repository, 2001.

Coté, Owen R., Jr. "The Politics of Innovative Military Doctrine: The U.S. Navy and Fleet Ballistic Missiles." PhD diss., Harvard University, February 1996.

Green, Andrew W. "It's Mine! Why the US Intelligence Community Does Not Share Information." Master's thesis, Air University, School of Advanced Air and Space Studies, July 2005.

Hayes-Roth, Rick, Curtis Blais, J. Mark Pullen, and Don Brutzman. "How to Implement National Information Sharing Strategy: Detailed Elements of the Evolutionary Management Approach Required." Monterey: Calhoun Institutional Archive of the Naval Postgraduate School, 2008.

Hesterman, Jennifer L. "Transnational Crime and the Criminal-Terrorist Nexus: Synergies and Corporate Trends." Master's thesis, Air University, April 2004.

Makarenko, Tamara. "The Crime-Terror Continuum: Modelling 21st Century Security Dynamics." PhD diss., University of Wales, Aberystwyth, 31 March 2005.

McDonald, Matthew F. "Joint Interagency Task Force-Illicit Trafficking: Enhancing the Interagency Organizational Framework for Operations along the Southwest Border." Master's thesis, US Marine Corps Command and Staff College, 1 May 2012.

Perry, Bruce H. "Information Sharing Among Intelligence, Law Enforcement, and Other Federal, State, and Local Agencies." Master's thesis, Air University, Air War College, 15 February 2008.

Remsing, Robert A. "'Seams' of Inefficiency and Joint Interagency Task Force (JIATF) Operations." Master's thesis, Naval War College, 16 May 2003.

Reinwald, Brian R. "Assessing the National Counterterrorism Center's Effectiveness in the Global War on Terror." Master's thesis, US Army War College, 6 March 2007.

Rivera, Reinaldo. "The Joint Interagency Task (JIATF) Conundrum: Cooperation among Competitors, is harmony achievable through trust and understanding?" Master's thesis, Naval War College, 3 February 2003.

Thuraisingham, Bhavani. "Information Sharing Strategies of the United States Federal Government and Its Allies And Our Contributions Towards Implementing These Strategies." Selected Papers in Security Studies: Volume 2, Technical Report UTDCS-23-10, Department of Computer Science, The University of Texas at Dallas, Dallas, 2 August 2010.

Articles

Carter, David L. and Jeremy G. Carter. "The Intelligence Fusion Process for State, Local and Tribal Law Enforcement." *Criminal Justice and Behavior* 36, no. 12 (December 2009): 1-39.

German, Michael and Jay Stanley. *What's Wrong with Fusion Centers?* New York: American Civil Liberties Union, December 2007.

Isacson, Adam, George Withers, and Joe Bateman. "An Uneasy Coexistence: security and migration along the El Paso-Ciudad Juarez border." Washington Office on Latin America, 20 December 2011, http://www.wola.org/commentary/an_uneasy_coexistence (accessed 24 February 2015).

Kavale, Stanley. "The Connection between Strategy and Structure." *International Journal of Business and Commerce* 1, no. 6 (February 2012): 59-70.

Kleiner, Art. "Chandler's Revolution." *Strategy + Business*, 9 April 2002, http://digitaledition.strategy-business.com/article/Professor+Chandler%E2%80%99s+Revolution/1482870/171835/article.html# (accessed 14 April 2015).

McChrystal, Stanley A. "It Takes a Network: The New Front Line of Modern Warfare." *Foreign Policy*, 21 February 2011, http://foreignpolicy.com/2011/02/21/it-takes-a-network/ (accessed 14 January 2015).

McConnell, Mike. "Overhauling Intelligence." *Foreign Affairs* 86, no. 4 (July/August 2007): 49-58.

Perry, Joseph and Cory Riesterer. "Joint Interagency Task Force South: Combating illicit drug operations." *Proceedings* 71, no. 3 (Fall 2014): 48-51.

Pope, Robert S. "Interagency Task Forces: The Right Tools for the Job." *Strategic Studies Quarterly* 5, no. 2 (Summer 2011): 113-152.

Stuhlreyer, Tom. "The JIATF Organization Model: Bringing the Interagency to Bear in Maritime Homeland Defense and Security." *Campaigning* (Spring 2007), 39-48.

Yeatman, Richard M. "JIATF-South: Blueprint for Success." *JFQ Forum* 42, no. 3 (2006): 26-27.

Books

Chandler, Alfred D., Jr. *Strategy and Structure: Chapters in the History of the Industrial Enterprise*. Cambridge: The M.I.T. Press, 1962.

Cornell, Svante and Michael Jonsson, ed. *Conflict, Crime, and the State in Postcommunist Eurasia*. Philadelphia: University of Pennsylvania Press, 2014.

Cronin, Audrey Kurth. *How Terrorism Ends: Understanding the Decline and Demise of Terrorist Campaigns*. Princeton: Princeton University Press, 2009.

Fishel, John T. "The Interagency Arena at the Operational Level: The Cases Now Known as Stability Operations," in *Affairs of State: The Interagency and National Security*, ed. Gabriel Marcella. Carlisle: Strategic Studies Institute, December 2008.

Lowenthal, Mark M. *Intelligence: From Secrets to Policy*. 2nd ed. Washington: CQ Press, 2003.

Gilman, Nils, Jesse Goldhammer, and Steven Weber. "Deviant Globalization," in *Convergence: Illicit Networks and National Security in the Age of Globalization*, ed. Michael Miklaucic and Jacqueline Brewer. Washington: National Defense University Press, 2013.

Munsing, Evan and Christopher J. Lamb. *Joint Interagency Task Force-South: The Best Known, Least Understood Interagency Success*. Washington: National Defense University Press, June 2011.

Nye, Joseph S., Jr., and David A. Welch. *Understanding Global Conflict and Cooperation: An Introduction to Theory and History*. 9th ed. Boston: Pearson, 2013.

Picard, Justin. "Can We Estimate the Global Scale and Impact of Illicit Trade?" in *Convergence: Illicit Networks and National Security in the Age of Globalization*, ed. Michael Miklaucic and Jacqueline Brewer. Washington: National Defense University Press, 2013.

Posen, Barry R. *The Sources of Military Doctrine: France, Britain, and Germany Between the World Wars*. Ithaca, NY: Cornell University Press, 1984.

Rosen, Stephen P. *Winning the Next War: Innovation and the Modern Military*. Ithaca, NY: Cornell University Press, 1991.

Schein, Edgar H. *Organizational Culture and Leadership*. 4th ed. San Francisco: Jossey-Bass, 2010.

Shelley, Louise I., John T. Picarelli, Allison Irby, Douglas M. Hart, Patricia A. Craig-Hart, Phil Williams, Steven Simon, Nabi Abdullaev, Bartosz Stanislawski, and Laura Covill. *Methods and Motives: Exploring Links between Transnational Organized Crime & International Terrorism*. Washington: Department of Justice, 23 June 2005.

Stavridis, James G. *Partnership for the Americas: Western Hemisphere Strategy and U.S. Southern Command*. Washington: National Defense University Press, 2010.

Surowiecki, James. *The Wisdom of Crowds*. New York: Anchor Books, 2005.

Wechsler, William F. and Gary Barnabo. "The Department of Defense's Role in Combating Transnational Organized Crime," in *Convergence: Illicit Networks and National Security in the Age of Globalization*, ed. Michael Miklaucic and Jacqueline Brewer. Washington: National Defense University Press, 2013.

Government Documents

2013-2015 National Counterterrorism Center Strategic Intent. Washington: National Counterterrorism Center, October 2012.

2014 National Network of Fusion Centers Final Report. Washington: Information Sharing Environment, January 2015.

2014-2017 National Strategy for the National Network of Fusion Centers. Washington: Information Sharing Environment, July 2014.

Department of Defense Counternarcotics & Global Threats Strategy. Washington: Deputy Assistant Secretary of Defense for Counternarcotics & Global Threats, 27 April 2011.

Department of Defense Directive (DODD) 8000.01, *Management of the Department of Defense Information Enterprise*, 10 February 2009.

Department of Defense Information Enterprise Strategic Plan, 2010-2012. Washington: Office of the Assistant Secretary of Defense for Networks and Information Integration/DOD Chief Information Officer, May 2010.

Department of Defense Information Sharing Implementation Plan. Washington: Office of the Assistant Secretary of Defense for Networks and Information Integration/DOD Chief Information Officer, April 2009.

Department of Defense Information Sharing Strategy. Washington: Department of Defense Information Sharing Executive, Office of the Chief Information Officer, 4 May 2007.

Department of Justice. *The Department of Justice's Terrorism Task Forces*. Washington: Office of the Inspector General, June 2005.

Department of Justice. *Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era*. Washington: Bureau of Justice Assistance, August 2006.

Department of Justice. *FY 2010 Performance and Accountability Report*. Washington: Office of the Attorney General, November 2010.

Department of Justice. *Review of the Drug Enforcement Administration's El Paso Intelligence Center*. Washington: Office of the Inspector General, June 2010.

Drug Enforcement Administration. "Intelligence Topics at DEA: El Paso Intelligence Center." http://www.dea.gov/ops/intel.shtml#EPIC (accessed 23 February 2015).

Drug Enforcement Administration Public Affairs. "'Project Below the Beltway' Targets Sinaloa and Juarez Cartels and Affiliated Violent Street Gangs Nationwide." 6 December 2012, http://www.dea.gov/divisions/hq/2012/hq120612.shtml (accessed 23 February 2015).

Federal Bureau of Investigation. "Protecting America from Terrorist Attack: Our Joint Terrorism Task Forces." http://www.fbi.gov/about-s/investigate/terrorism/terrorism_jttfs (accessed 19 March 2015).

Federal Bureau of Investigation. "Italian Organized Crime." http://www.fbi.gov/about-us/investigate/organizedcrime/italian_mafia (accessed 3 December 2014).

Government Accountability Office. *Information Sharing: DHS is Assessing Fusion Center Capabilities and Results, but Needs to More Accurately Account for Federal Funding Provided to Centers*, GAO-15-155. Washington: Government Accountability Office, November 2014.

Government Accountability Office. *Interagency Collaboration: Key Issues for Congressional Oversight of National Security Strategies, Organizations, Workforce, and Information Sharing*, GAO-09-904SP. Washington: Government Accountability Office, September 2009.

Government Accountability Office. *Report to the Co-Chairman, Caucus on International Narcotics Control, U.S. Senate: Drug Control, Better Coordination with the Department of Homeland Security and an Updated Accountability Framework Can Further Enhance DEA's Efforts to Meet Post-9/11 Responsibilities*, GAO-09-63. Washington: Government Accountability Office, March 2009.

Inspectors General of the Intelligence Community, Central Intelligence Agency, Department of Justice, and Department of Homeland Security. *Unclassified Summary of Information Handling and Sharing Prior to the April 15, 2013 Boston Marathon Bombings*. Washington: Intelligence Community, 10 April 2014.

Joint Interagency Task Force South. "Command Group." http://www.jiatfs.southcom.mil/index-1.aspx (accessed 24 February 2015).

Joint Interagency Task Force South. "Joint Interagency Task Force South: Serving the Nation for Over 20 Years." http://www.jiatfs.southcom.mil/index.aspx (accessed 24 February 2015).

National Counterterrorism Center. "Overview." http://www.nctc.gov/overview.html (accessed 21 March 2015).

National Counterterrorism Center. "Who We Are." http://www.nctc.gov/whoweare.html (accessed 21 March 2015).

The National Military Strategy of the United States of America. Washington: The Chairman of the Joint Chiefs of Staff, February 2011.

The National Security Strategy of the United States of America. Washington: The White House, May 2010.

National Southwest Border Counternarcotics Strategy. Washington: Office of National Drug Control Policy, 2013.

National Strategy for Information Sharing and Safeguarding. Washington: The White House, December 2012.

Strategy to Combat Transnational Organized Crime: Addressing Converging Threats to National Security. Washington: The White House, July 2011.

Strategic Implementation Plan for the National Strategy for Information Sharing and Safeguarding. Washington: National Security Staff, December 2013.

Sustaining Global Leadership: Priorities for 21st Century Defense. Washington: Secretary of Defense, January 2012.

US House of Representatives. *Majority Staff Report on the National Network of Fusion Centers*. Washington: Committee on Homeland Security, July 2013.

US Senate. *Federal Support for and Involvement in State and Local Fusion Centers*. Washington: Permanent Subcommittee on Investigations, 3 October 2012.

US Senate. *Unclassified Executive Summary of the Committee Report on the Attempted Terrorist Attack on Northwest Airlines Flight 253*. Washington: Select Committee on Intelligence, 18 May 2010.

Reports

The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States. Washington: National Commission on Terrorist Attacks Upon the United States, 2004.

Best, Richard A., Jr. *The National Counterterrorism Center (NCTC)—Responsibilities and Potential Congressional Concerns*, CRS Report R41022. Washington: Congressional Research Service, 19 December 2011.

Bjelopera, Jerome P. and Kristin M. Finklea. *Organized Crime: An Evolving Challenge for U.S. Law Enforcement*, CRS Report R41547. Washington: Congressional Research Service, 6 January 2012.

Finklea, Kristin M. *Organized Crime in the United States: Trends and Issues for Congress*, CRS Report R40525. Washington: Congressional Research Service, 22 December 2010.

The Globalization of Crime: A Transnational Organized Crime Threat Assessment. Vienna, Austria: United Nations Office on Drugs and Crime, 2010.

Masse, Todd, Siobhan O'Neil, and John Rollins. *Fusion Centers: Issues and Options for Congress*, CRS Report RL34070. Washington: Congressional Research Service, 6 July 2007.

Rollins, John and Liana Sun Wyler. *Terrorism and Transnational Crime: Foreign Policy Issues for Congress*, CRS Report R41004. Washington: Congressional Research Service, 11 June 2013.

United Nations Convention Against Transnational Organized Crime and the Protocols Thereto. Vienna, Austria: United Nations Office on Drugs and Crime, 2004.

Speeches

Posture Statement of General Douglas M. Fraser, Commander, US Southern Command, before the Armed Services Committee, US House of Representatives, 6 March 2012.

Statement of Derek S. Maltz, Special Agent in Charge, Special Operations Divisions, Drug Enforcement Administration, before the Subcommittee on Terrorism, Nonproliferation, and Trade, Committee on Foreign Affairs, US House of Representatives, "Narcoterrorism and the Long Reach of U.S. Law Enforcement, Part II," 17 November 2011.

Statement of the Honorable Michele Leonhart, Administrator, Drug Enforcement Administration, before the Subcommittee on Commerce, Justice, Science and Related Agencies, Committee on Appropriations, US House of Representatives, 2 April 2014.

Statement of the Honorable Paul Stockton, Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs, before the Subcommittee on Border and Maritime Security, Committee on Homeland Security, US House of Representatives, 17 April 2012.

Villalobos, Larry and Carlos Almengor. "DEA Museum Lecture Series – An Overview of the El Paso Intelligence Center." 1 December 2011, http://www.deamuseum.org/ education/transcripts/ EPIC-120111.pdf (accessed 26 February 2015).

Wechsler, William F., Deputy Assistant Secretary of Defense for Counternarcotics and Global Threats, Department of Defense. Address to The Washington Institute for Near East Policy, Washington, 26 April 2012.